Lantech

IES-22812F-2P

12 100FX + 8 10/100TX + 2 1000 SFP Industrial Power station L2 Plus Managed Switch

User Manual

V1.01

Nov-2010

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

Chapter 1 Introduction 1

1.1 Hardware Features 1

1.2 Software Features 2

1.3 Package Contents 4

Chapter 2 Hardware Description 5

2.1 Physical Dimensions 5

2.2 Front (LED) Panel 5

2.3 Rear Panel 6

2.4 LED Indicators 7

Chapter 3 Hardware Installation 9

3.1 Rack-mounted Installation 9

3.2 Cabling 11

3.3 Wiring the Power Inputs 14

3.4 Wiring the P-Fail Alarm Contact 15

Chapter 4 Network Application 16

4.1 X-Ring Application 17

4.2 Coupling Ring Application 18

4.3 Dual Homing Application 19

Chapter 5 Console Management 20

5.1 Connecting to the Console Port 20

5.2 Pin Assignment 20

5.3 Login in the Console Interface 21

5.4 CLI Management 22

5.5 Commands Level 22

Chapter 6 Web-Based Management..... 24

6.1 About Web-based Management 24

6.2 Preparing for Web Management 24

6.3 System Login..... 25

6.4 System Information 26

6.5 IP Configuration..... 27

6.6 DHCP Server..... 28

6.6.1 System configuration..... 29

6.6.2 Client Entries..... 30

6.6.3 Port and IP Bindings..... 31

6.7 TFTP 32

6.7.1 Update Firmware..... 32

6.7.2 Restore Configuration 33

6.7.3 Backup Configuration..... 34

6.8 System Event Log 35

6.8.1 Syslog Configuration 35

6.8.2 System Event Log—SMTP Configuration..... 37

6.8.3 System Event Log—Event Configuration..... 39

6.9 Fault Relay Alarm..... 41

6.10 SNTP Configuration 42

6.11 IP Security..... 46

6.12 User Authentication..... 48

6.13 Advanced Configuration..... 49

6.13.1 Broadcast Storm Filter..... 49

6.13.2 Aging Time 51

6.13.3 Jumbo Frame 52
6.14 Port Statistics 53
6.15 Port Counters 55
6.16 Port Control 58
6.17 Port Trunk.....60
6.17.1. Aggregator setting 60
6.17.2. Aggregator Information 62
6.17.3. State Activity.....66
6.18 Port Mirroring.....68
6.19 Rate Limiting 69
6.20 VLAN configuration 70
6.20.1. Port-based VLAN.....70
6.20.2. 802.1Q VLAN 74
6.21 Rapid Spanning Tree 79
6.21.1. System Configuration 79
6.21.2. Port Configuration.....81
6.22 SNMP Configuration.....83
6.22.1. System Configuration 83
6.22.2. Trap Configuration.....85
6.22.3. SNMPV3 Configuration.....86
6.23 QoS Configuration.....89
6.24 IGMP Configuration.....91
6.25 X-Ring 93
6.26 LLDP Configuration.....95
6.27 Security—802.1X/Radius Configuration.....96
6.27.1. System Configuration 96
6.27.2. Port Configuration.....97

6.27.3. Misc Configuration 98
6.28 MAC Address Table 100
6.28.1. Static MAC Address 100
6.28.2. MAC Filtering 102
6.28.3. All MAC Addresses 103
6.28.4. MAC Address Table—Multicast Filtering 104
6.29 Access Control List 106
6.30 Factory Default 107
6.31 Save Configuration 108
6.32 System Reboot 109
Troubleshooting 110
Appendix A — RJ-45 Pin Assignment 111
Appendix B — Command Sets 114
Commands Set List 114
System Commands Set 114
Port Commands Set 118
Trunk Commands Set 120
VLAN Commands Set 122
Spanning Tree Commands Set 124
QOS Commands Set 127
IGMP Commands Set 128
Mac / Filter Table Commands Set 129
SNMP Commands Set 131
Port Mirroring Commands Set 134
802.1x Commands Set 135
TFTP Commands Set 138
SystemLog, SMTP and Event Commands Set 139

SNTP Commands Set 142
X-Ring Commands Set.....144
LLDP Command Set.....145
Access Control List Command Set 146

Chapter 1 Introduction

The IES-22812F-2P is a cost-effective solution and meets the high reliability requirements demanded by industrial applications. The IES-22812F-2P can be easily managed through the Web GUI. Using fiber port can extend the connection distance that increases the network elasticity and performance. It provides the X-Ring function that can prevent the network connection failure, and meets the standard of IEC-61850-3 and IEEE-1613 for the substation environment applications.

1.1 Hardware Features

Switch Architecture	Back-plane (Switching Fabric): 8Gbps Packet throughput ability(Full-Duplex): 11.9Mpps @64bytes
Transfer Rate	14,880pps for Ethernet port 148,800pps for Fast Ethernet port 1,488,000pps for Gigabit Fiber Ethernet port
Packet Buffer	4Mbits
Mac Address	8K MAC address table
Flash ROM	4Mbytes
DRAM	64Mbytes
Jumbo Frame	9022bytes (for Gigabit ports)
Connector	10/100TX: 8 x RJ-45 100FX : 12 x SC Gigabit Mini-GBIC: 2 x Mini-GBIC sockets Console port: RJ-45 type
Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5/5E cable EIA/TIA-568 100-ohm (100m)
Optical Cable	Multi-mode: 50/125um~62.5/125um Single-mode: 9/125um
Protocol	CSMA/CD
LED	***Front Panel*** Per unit: Power 1 (Green), Power 2 (Green), P-Fail (Red),

	R.Master (Green) Port1~22 : Link/Activity (Green), Port13~20: 100M (Green) ***Rear Panel*** Per unit: Power 1 (Green), Power 2 (Green), P-Fail (Red), R.Master (Green) Port1~22 : Link/Activity (Green), Port13~20: Full-duplex (Amber)
Reverse Polarity Protection	Present
Overload Current Protection	Present
Power Supply	IES-22812F-2P: 100~240$V_{AC/DC}$
Power Consumption	IES-22812F-2P: 27.6 Watts max. @ 110 V_{DC} 26.2 Watts max. @ 110 V_{AC}
Operating Humidity	5% to 95% (Non-condensing)
Operating Temperature	Wide Operating Temperature (-40℃~85℃)
Storage Temperature	-40℃ to 85℃
Case Dimensions	Metal case. IP-30, 440mm (W) x 44mm (H) x 280mm (D)
Installation	DIN-rail and Wall-mount Design

1.2 Software Features

Management	SNMP v1 v2c, v3 / Web / Telnet / CLI
SNMP MIB	RFC 1215 Trap, RFC1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643 , RFC 1757, RSTP MIB, LLDP MIB, Private MIB
VLAN	Port Based VLAN IEEE 802.1Q Tag VLAN (256 entries)/ VLAN ID (Up to 4K, VLAN ID can be assigned from 1 to 4094.) GVRP (256 Groups)
Port Trunk with LACP	LACP Port Trunk: 13 Trunk groups/Maximum 4 trunk members
LLDP	Support LLDP to allow switch to advise its identification and capability on the LAN
Spanning Tree	Support IEEE802.1w Rapid Spanning Tree
X-Ring	Support X-Ring, Dual Homing, Couple Ring Topology.

	Provide redundant backup feature and the recovery time below 20ms.
Quality of Service	The quality of service determined by port, Tag and IPv4 Type of service, IPv4 Different Service
Class of Service	Support IEEE802.1p class of service, per port provides 4 priority queues
Port Security	Support 50 entries of MAC address for static MAC and another 50 for MAC filter
Port Mirror	Support 3 mirroring types: “RX, TX and Both packet”.
IGMP	Support IGMP snooping v1,v2 256 multicast groups and IGMP query
IP Security	Support 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder.
Login Security	Support IEEE802.1x Authentication/RADIUS
Bandwidth Control	Support ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 0~100Mbps for Port1~20 and 0~1000Mbps for Port21/22.
Flow Control	Support Flow Control for Full-duplex and Back Pressure for Half-duplex
System Log	Support System log record and remote system log server
SMTP	Support SMTP Server and 6 e-mail accounts for receiving event alert
Relay Alarm	Provides one relay output for port breakdown & power failure Alarm Relay current carrying ability: 1A @ DC24V
SNMP Trap	Up to 3 Trap stations Cold start, Warm start, Port link up, Port link down, Authentication Failure, Port fault relay alarm, X-Ring topology change
DHCP	Provide DHCP Client/ DHCP Server functions
DNS	Provide DNS client feature and support Primary and Secondary DNS server
SNTP	Support SNTP to synchronize system clock in Internet
Firmware Update	Support TFTP firmware update, TFTP backup and restore.
Configuration Upload and Download	Support binary configuration file for system quick installation
ifAlias	Each port allows an alphabetic string of 128-byte assigned

	as its own unique name via the CLI or SNMP interface.

1.3 Package Contents

Please refer to the package content list below to verify them against the checklist.

- IES-22812F-2P x 1
- User manual x 1
- Mounting plate x 2
- RJ-45 to DB9-Female cable x 1

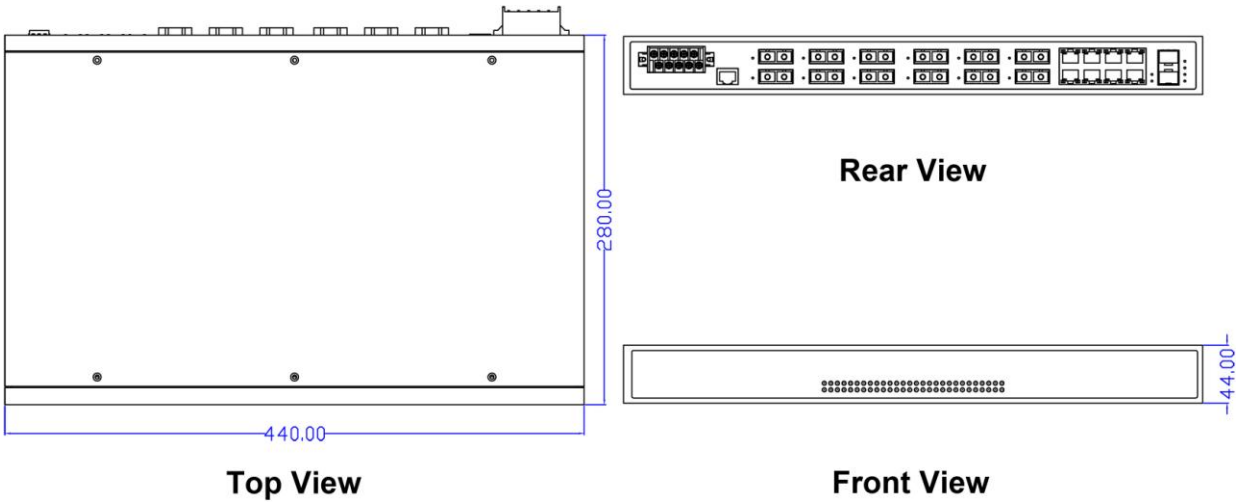
Compare the contents of the industrial switch with the standard checklist above. If any item is damaged or missing, please contact the local dealer for service.

Chapter 2 Hardware Description

In this paragraph, we will describe the Industrial switch's hardware spec, port, cabling information, and wiring installation.

2.1 Physical Dimensions

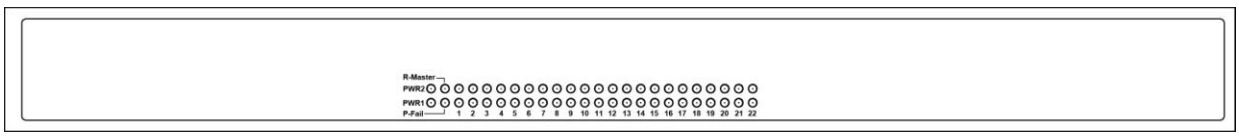
IES-22812F-2P dimensions (W x H x D) are **440mm x 44mm x 280mm** as the figure shown below.



Mechanical Dimensions

2.2 Front (LED) Panel

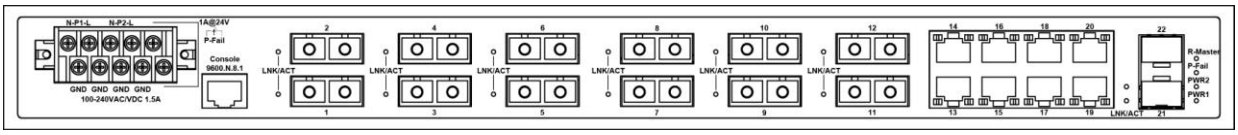
The figure below illustrates the front panel of the IES-22812F-2P.



Front Panel of the industrial switch

2.3 Rear Panel

The 12 fiber ports, 8 copper ports, 2 SFP ports, console port and terminal block are located on the rear panel of the Managed Industrial Switch.



Front Panel of the industrial switch

2.4 LED Indicators

The diagnostic LED indicators located on the front panel & rear panel of the industrial switch provide real-time information of the system and optional status. The following table provides description of the LED status and their meanings for the switch.

Front Panel			
LED	**Color**	**Status**	**Meaning**
R.M.	Green	On	The switch is the **MASTER** device of the X-Ring group
		Off	The switch is not the **MASTER** device of the X-Ring group
P-Fail	Red	On	● Power1 is inactive ● Power2 is inactive ● Port Link-down ● Port Link-broken
		Off	No failure occurs
P1	Green	On	Power 1 is active
		Off	Power 1 is inactive
P2	Green	On	Power 2 is active
		Off	Power 2 is inactive
SPD	Green	On	1000M (21, 22) 100M (1 ~ 20)
		Off	10M (13 ~ 20)
LNK/ACT	Green	On	The port is connected to network
		Blinking	Packet transmitting/receiving
		Off	Not connected to network

Rear Panel

LED	Color	Status	Meaning
R.M.	Green	On	The switch is the **MASTER** device of the X-Ring group
		Off	The switch is not the **MASTER** device of the X-Ring group
P-Fail	Red	On	● Power1 is inactive ● Power2 is inactive ● Port Link-down ● Port Link-broken
		Off	No failure occurs
P1	Green	On	Power 1 is active
		Off	Power 1 is inactive
P2	Green	On	Power 2 is active
		Off	Power 2 is inactive
LNK/ACT (Port 1~22)	Green	On	The port is connected to network
		Blinking	Packet transmitting/receiving
		Off	Not connected to network
FDX (Port 13~20)	Amber	On	Full-duplex
		Off	Half-duplex

Chapter 3 Hardware Installation

3.1 Rack-mounted Installation

The IES-22812F-2P comes with a rack-mounted kit and can be mounted in an EIA standard size, 19-inch Rack. The Switch can be placed in a wiring closet with other equipment.

Perform the following steps to rack mount the switch:

A. Position one bracket to align with the holes on one side of the switch and secure it with the smaller bracket screws. Then attach the remaining bracket to the other side of the Switch.

Figure 2-4. Attach mounting brackets with screws

B. After attaching the mounting brackets, position the IES-22812F-2P in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the Switch to the rack by a screwdriver with the rack-mounting screws.

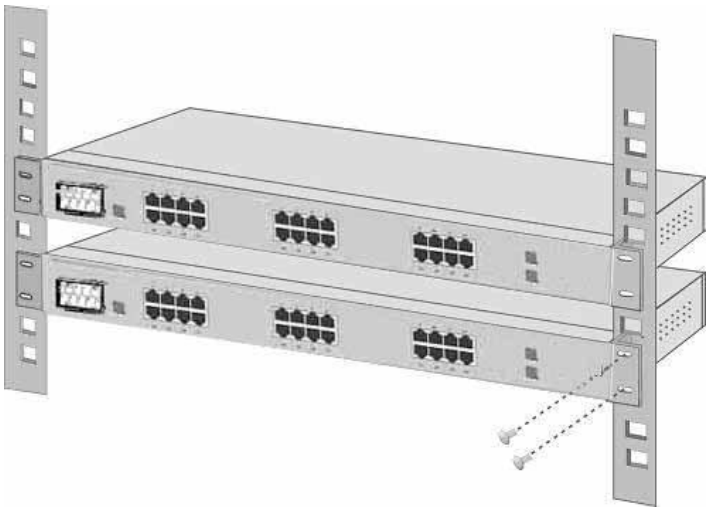


Figure 2-5. Mount the Switch in 19” Rack

Note: For proper ventilation, allows about at least 4 inches (10 cm) of clearance on the front and 3.4 inches (8 cm) on the back of the Switch. This is especially important for enclosed rack installation.

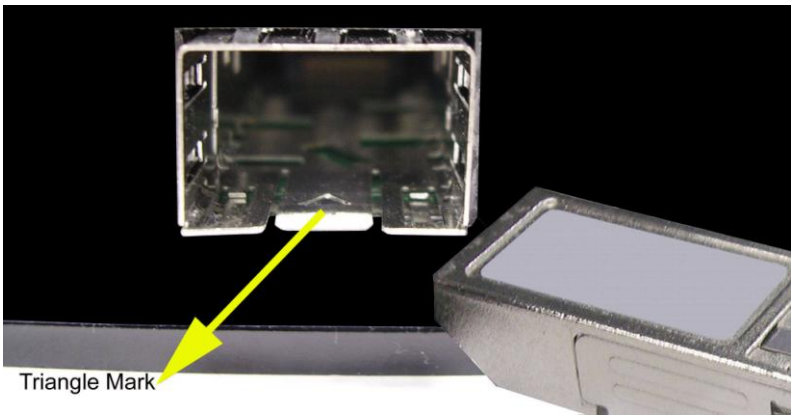
3.2 Cabling

Twisted-pair segment can be established by using unshielded twisted pair (UTP) or shielded twisted pair (STP) cabling. The cable between the link partner (switch, hub, workstation, etc.) and the switch must be less than 100 meters (328 ft.) long and comply with the IEEE 802.3ab 1000Base-T standard for Category 5e or above.

The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communication applications. Please note that you must use the class I optical transceivers which conform to U.S. code of federal regulation, 21 CFR 1040.

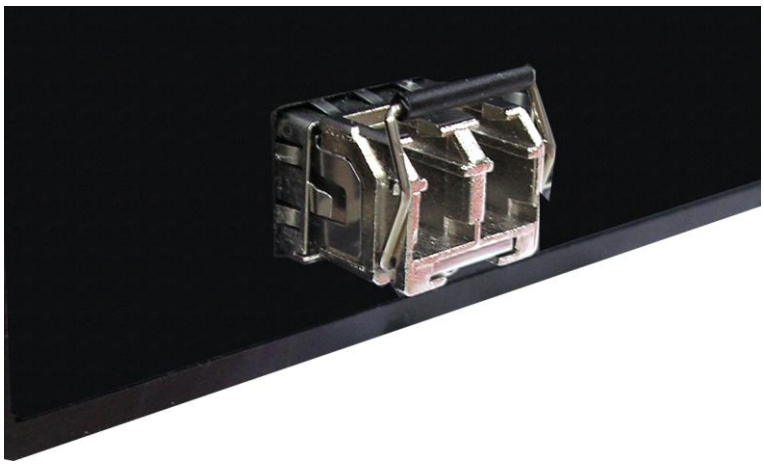
To connect the transceiver and LC cable, please follow the steps shown as below:

First, insert the transceiver into the mini-GBIC slot. Notice that the triangle mark indicates bottom of the slot.



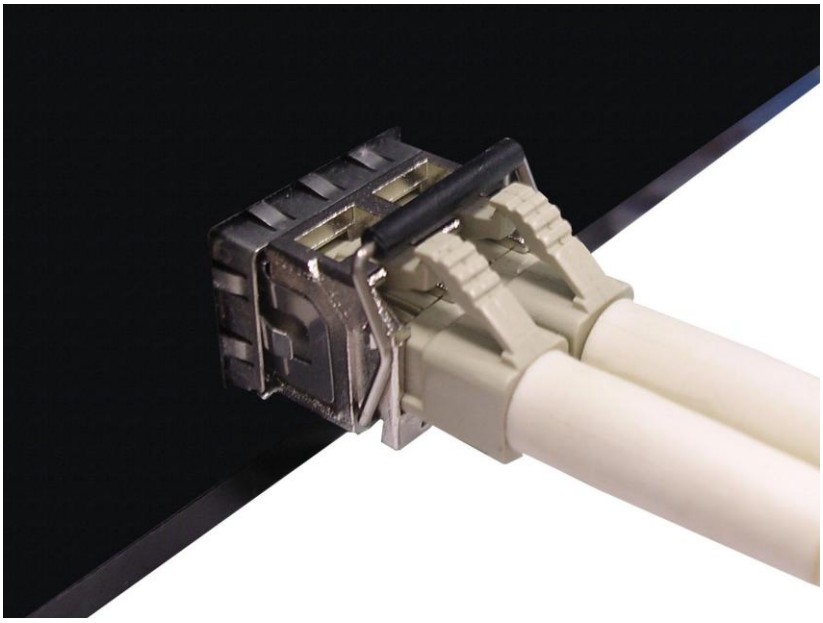
Transceiver to the SFP slot

Make sure the transceiver is aligned correctly and then slide it into the mini-GBIC slot until a click is heard.



Transceiver Inserted

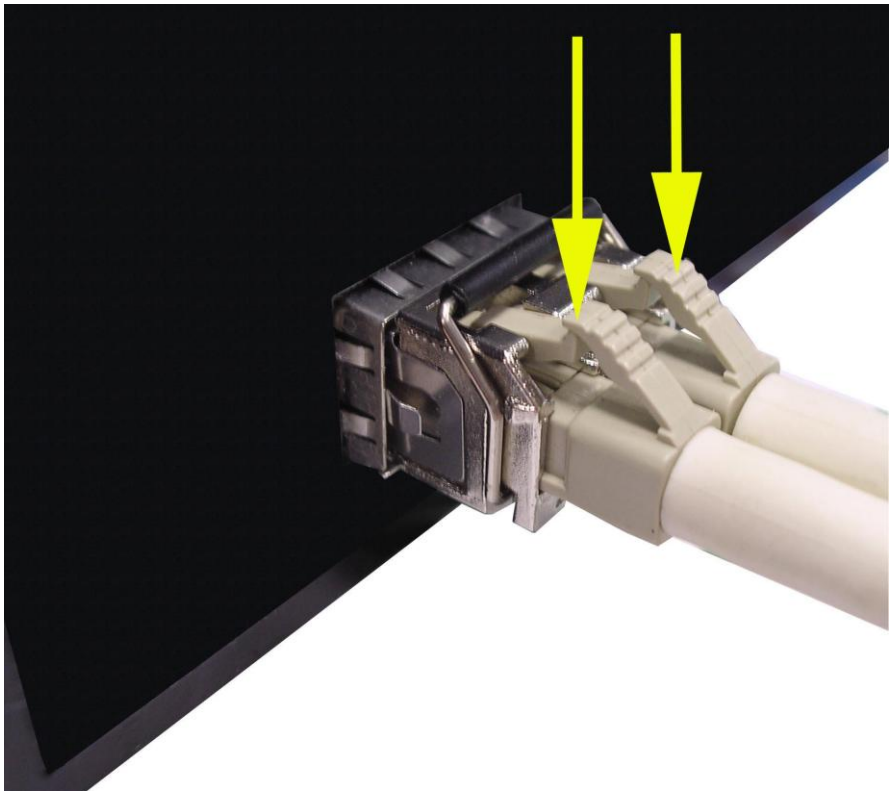
Second, insert the fiber cable of LC connector into the transceiver.



LC connector to the transceiver

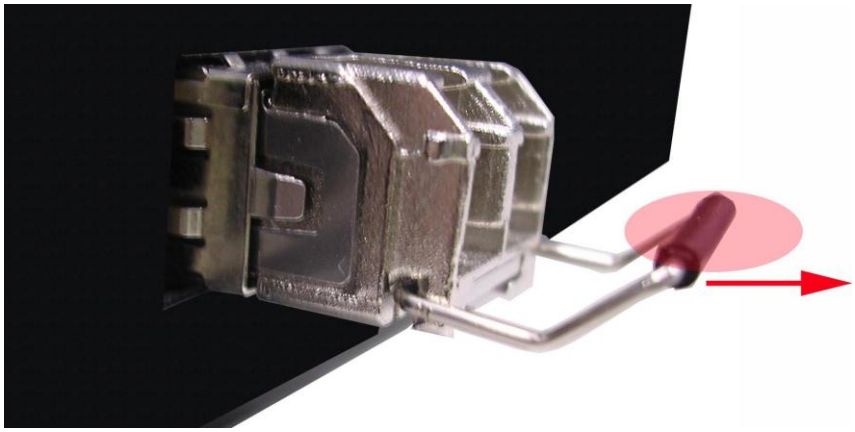
To remove the LC connector from the transceiver, please follow the steps shown below:

First, press the upper side of the LC connector from the transceiver and pull it out to release.



Remove LC connector

Second, push down the metal loop and pull the transceiver out by the plastic part.



Transceiver pulled out from the SFP slot

3.3 Wiring the Power Inputs

Please follow the steps below to insert the power wires.

IES-22812F-2P power inputs wiring

1. Attach AC or DC power wires to the contacts.

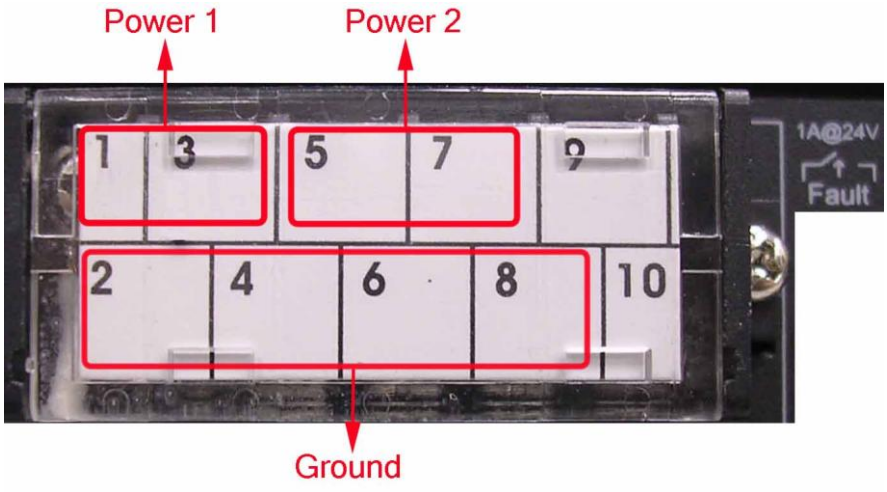
   Power 1: Pin 1 (**-**), Pin 3 (**+**) for **DC** power source

   Pin 1 (**N**), Pin 3 (**L**) for **AC** power source

   Power 2: Pin 5 (**-**), Pin 7 (**+**) for **DC** power source

   Pin 5 (**N**), Pin 7 (**L**) for **AC** power source

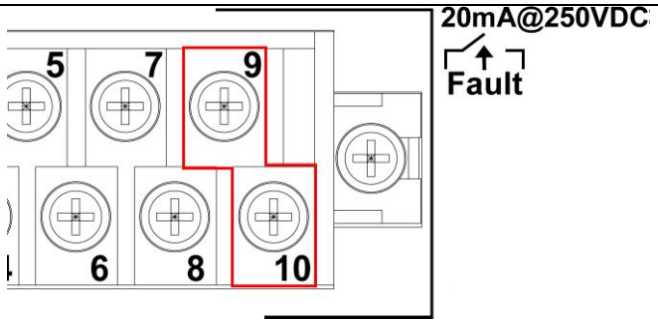
   Ground: Pin 2, 4, 6 and 8



2. Tighten the wire-clamp screws to prevent the wires from loosing.

3.4 Wiring the P-Fail Alarm Contact

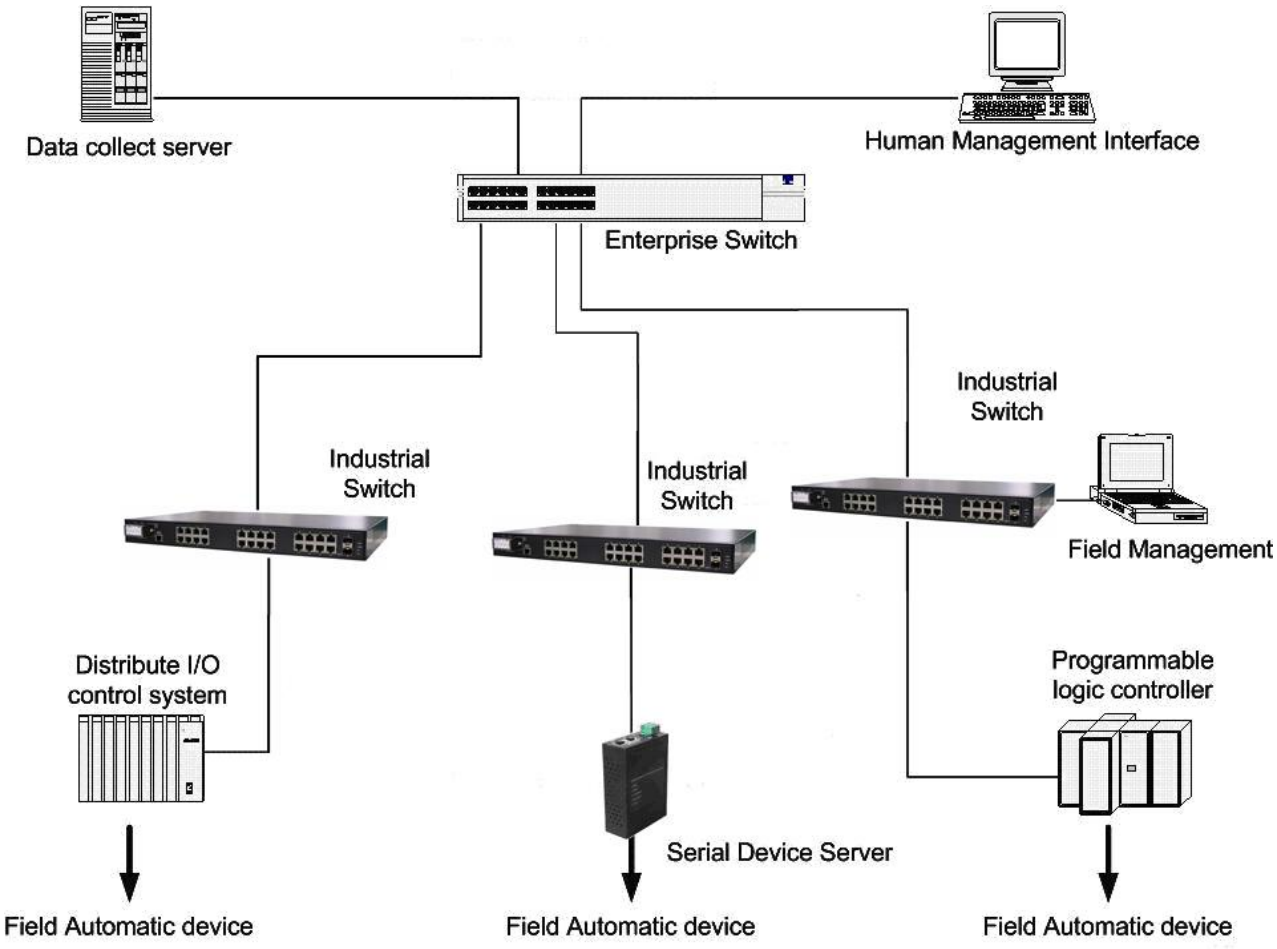
Attach the wires to form a ***Normally Close*** circuit. When power or network linking failure occurs, the system will break the circuit to ***Open*** status. Please refer to the figure illustrated below.



IES-22812F-2P P-Fail Alarm connectors

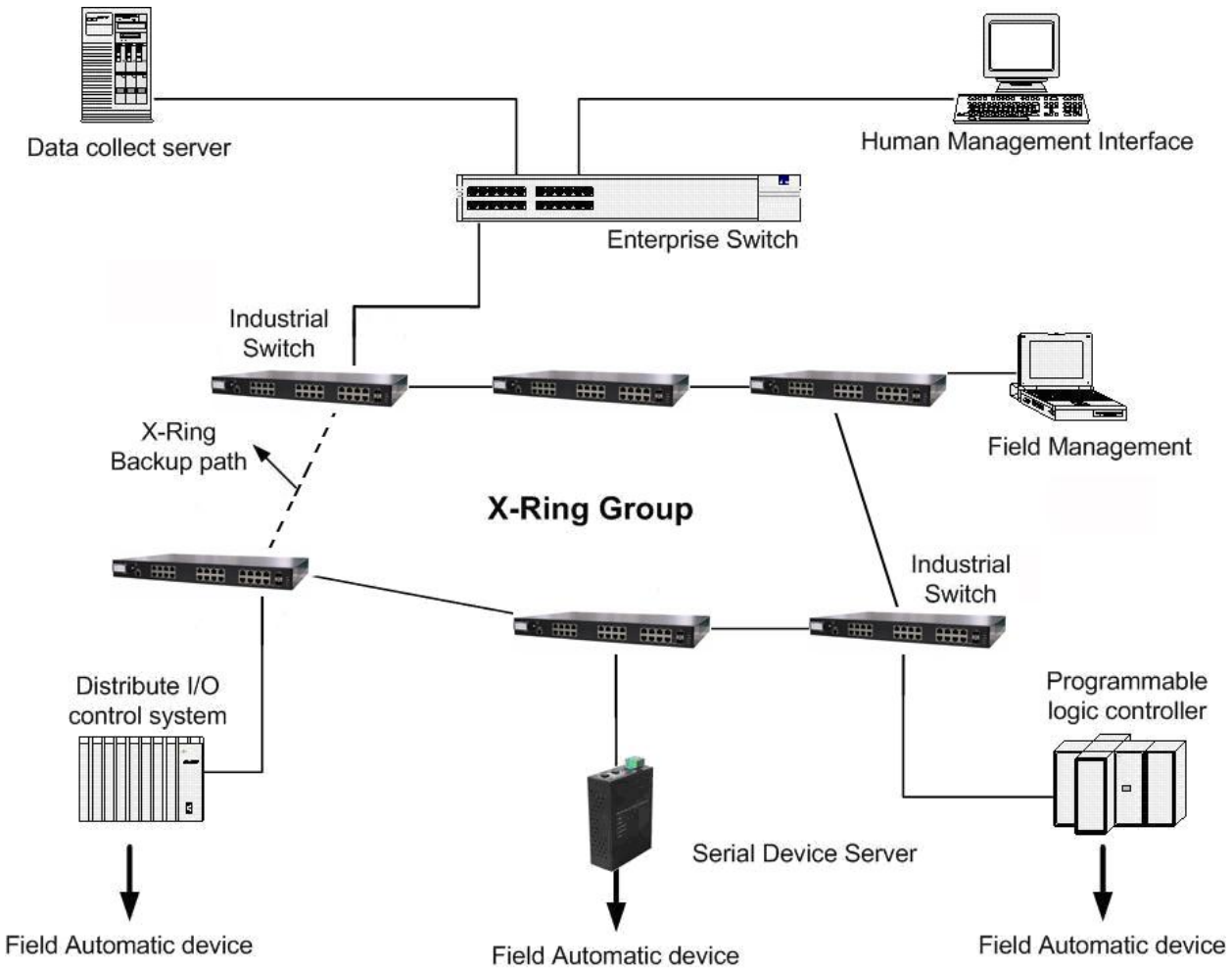
Chapter 4 Network Application

This chapter provides some sample applications to help the user to have more actual idea of industrial switch function application. A sample application of the industrial switch is shown as below:



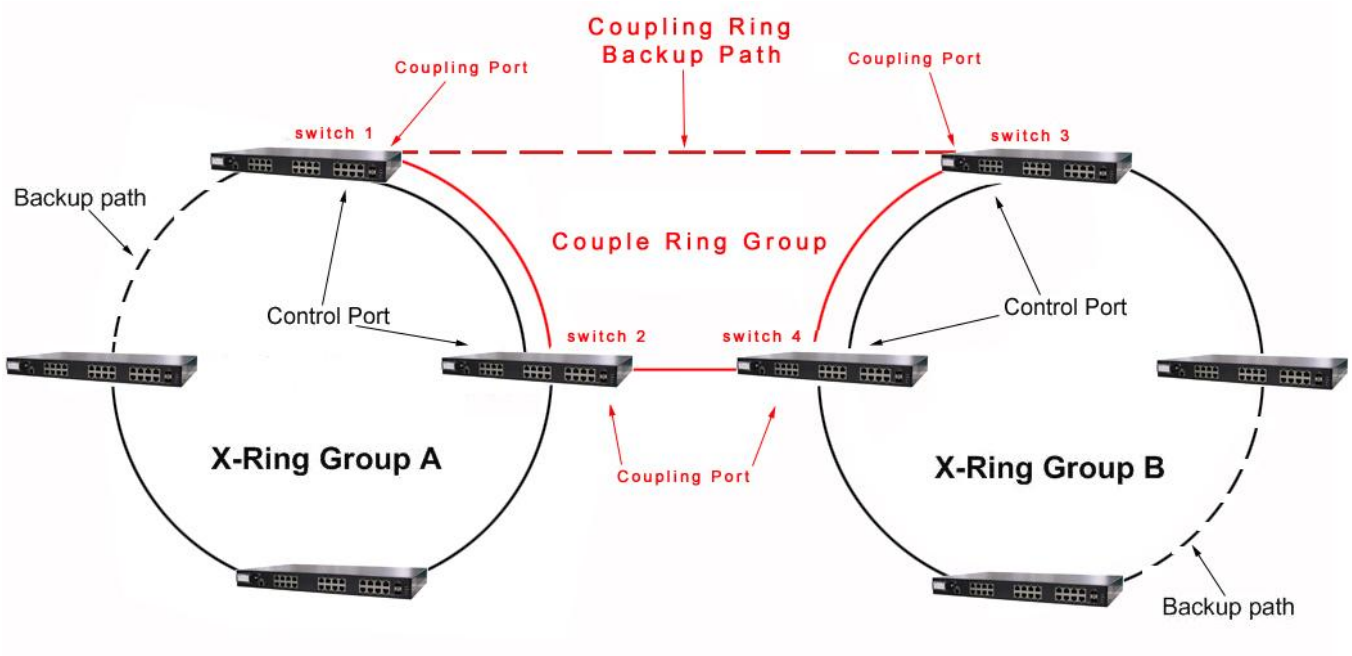
4.1 X-Ring Application

The industrial switch supports the X-Ring protocol that can help the network system to recover from network connection failure within 20ms or less, and make the network system more reliable. The X-Ring algorithm is similar to Spanning Tree Protocol (STP) and Rapid STP (RSTP) algorithm but its recovery time is less than STP/RSTP. The figure below is a sample of X-Ring application.



4.2 Coupling Ring Application

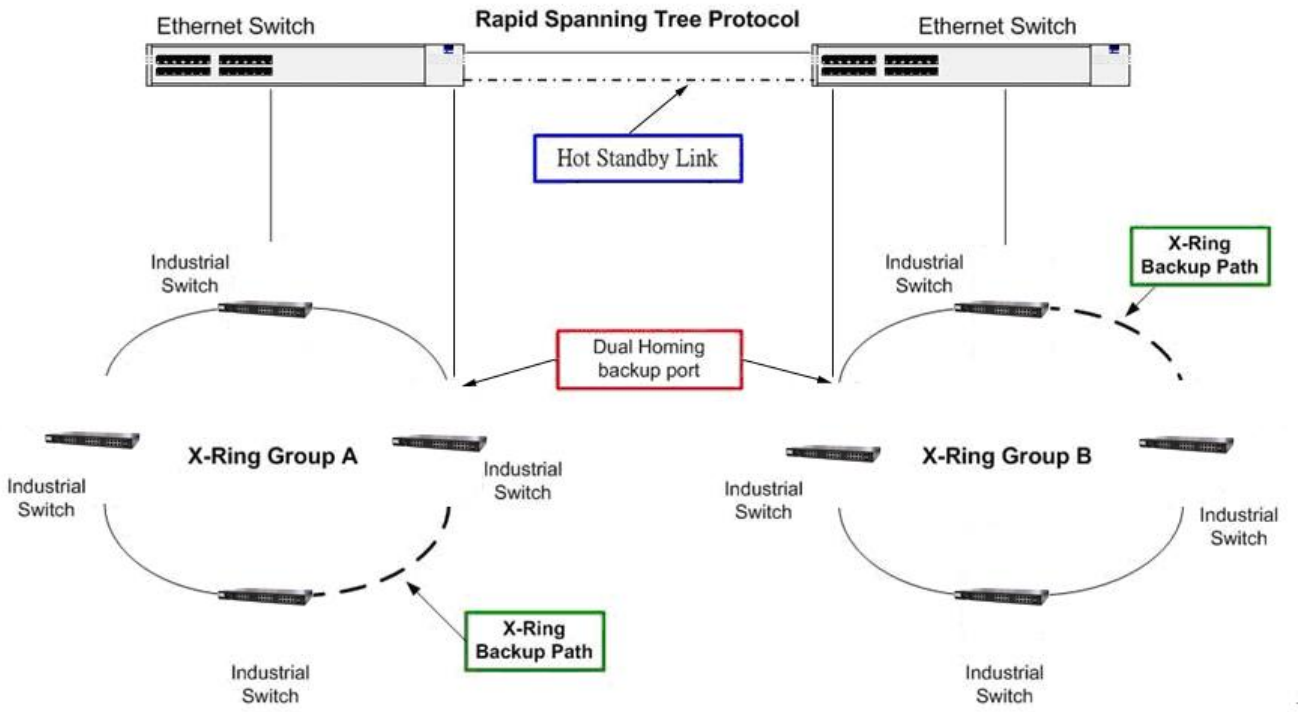
In the network, it may have more than one X-Ring group. Using the coupling ring function can connect each X-Ring for the redundant backup. It can ensure the transmissions between two ring groups not to fail. The following figure is a sample of coupling ring application.



4.3 Dual Homing Application

Dual Homing function is to prevent the connection loss from between X-Ring group and upper level/core switch. Assign two ports to be the Dual Homing port that is backup port in the X-Ring group. The Dual Homing function only works when the X-Ring function is active. Each X-Ring group only has one Dual Homing port.

[NOTE] *In Dual Homing application architecture, the upper level switches need to enable the Rapid Spanning Tree protocol.*

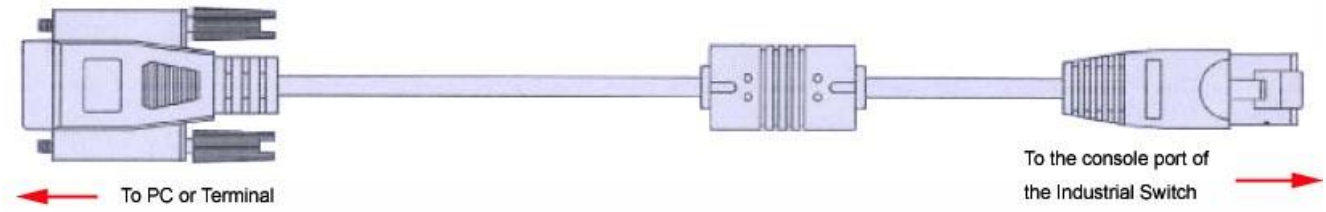


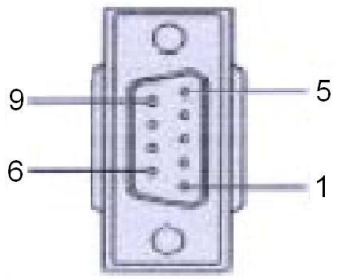
X-Ring I Recovery time table	X- Ring	Couple Ring	Dual Homing
Recovery Time(ms) (Using 1G Fiber Cable or 100Mb Copper Cable)	10	150	150~6000
Recovery Time(ms) (Using 1G Coppor Cable)	150	150	150~6000

Chapter 5 Console Management

5.1 Connecting to the Console Port

The supplied cable which one end is RS-232 connector and the other end is RJ-45 connector. Attach the end of RS-232 connector to PC or terminal and the other end of RJ-45 connector to the console port of the switch. The connected terminal or PC must support the terminal emulation program.





DB 9-pin Female

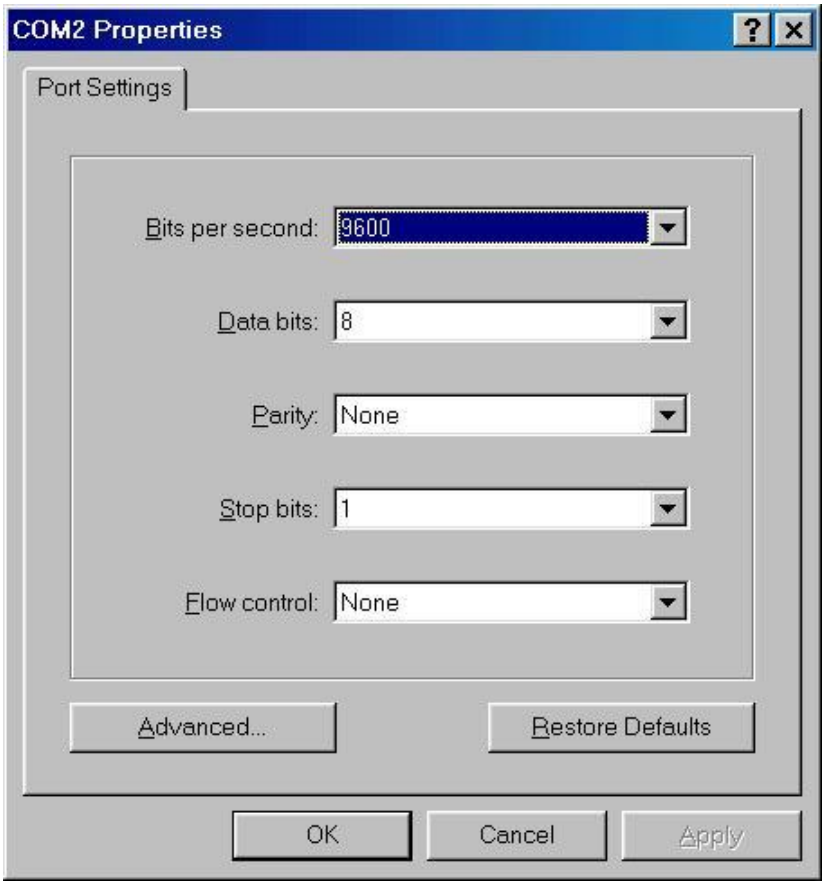
5.2 Pin Assignment

DB9 Connector	RJ-45 Connector
NC	1 Orange/White
2	2 Orange
3	3 Green/White
NC	4 Blue
5	5 Blue/White
NC	6 Green
NC	7 Brown/White
NC	8 Brown

5.3 Login in the Console Interface

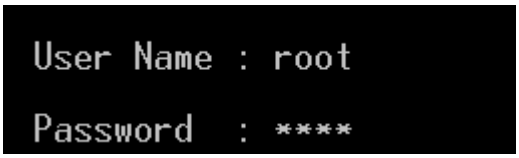
When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None



The settings of communication parameters

After finishing the parameter settings, click '**OK**'. When the blank screen shows up, press **Enter** key to have the login prompt appears. Key in '**root**' (default value) for both User name and Password (use **Enter** key to switch), then press **Enter** key and the Main Menu of console management appears.



Console login interface

5.4 CLI Management

The system supports the console management—CLI command. After you log in on to the system, you will see a command prompt. To enter CLI management interface, type in "**enable**" command.

CLI command interface

The following table lists the CLI commands and description.

5.5 Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. • Display system

				information.
Privileged EXEC	Enter the **enable** command while in User EXEC mode.	switch#	Enter **disable** to exit.	The privileged command is the advanced mode. Use this mode to • Display advanced function status • Save configuration
Global Configuration	Enter the **configure** command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter **exit** or **end**	Use this mode to configure those parameters that are going to be applied to your switch.
VLAN database	Enter the **vlan database** command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface of fast Ethernet command (with a specific interface) while in global configuration mode	switch (config-if)#	To exit to global configuration mode, enter **exit**. To exit to privileged EXEC mode, enter **exit** or **end**.	Use this mode to configure parameters for the switch and Ethernet ports.

Chapter 6 Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

6.1 About Web-based Management

There is an embedded HTML web site residing in flash memory on CPU board of the switch, which offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0 or later version. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

6.2 Preparing for Web Management

Before using the web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser. The industrial switch default value of IP, subnet mask, username and password are listed as below:

- IP Address: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
- User Name: **root**
- Password: **root**

6.3 System Login

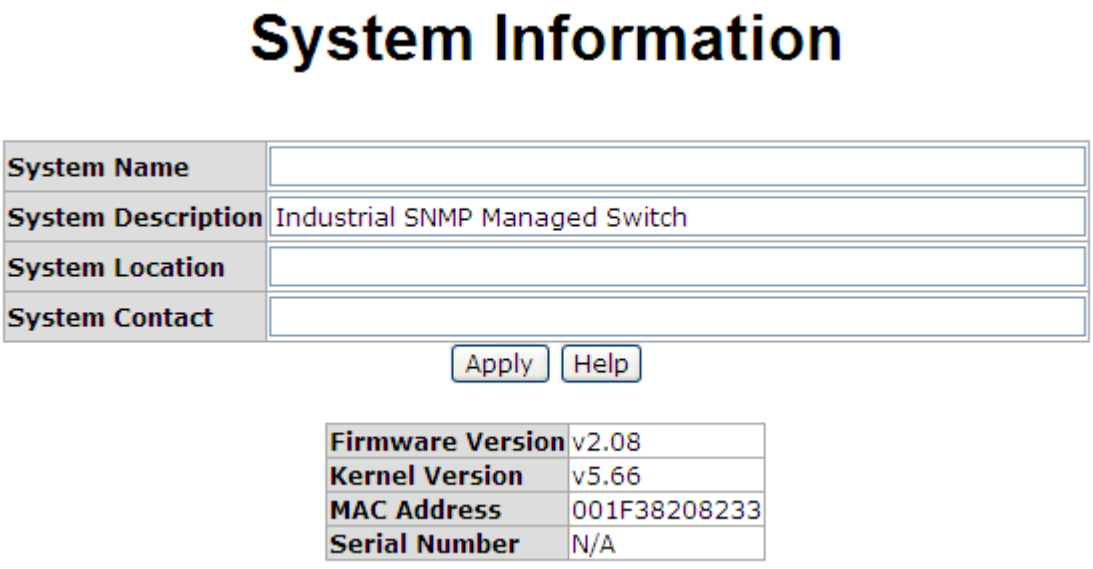
1. Launch the Internet Explorer on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.

3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as ‘**root**’.
5. Press **Enter** or click the **OK** button, and then the home screen of the Web-based management appears.

6.4 System Information

User can assign the system name, description, location and contact personnel to identify the switch. The version table below is a read-only field to show the basic information of the switch.

- **System Name:** Assign the system name of the switch (The maximum length is 64 bytes)
- **System Description:** Describes the switch.
- **System Location:** Assign the switch physical location (The maximum length is 64 bytes).
- **System Contact:** Enter the name of contact person or organization.
- **Firmware Version:** Displays the switch's firmware version
- **Kernel Version:** Displays the kernel software version
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default)
- And then, click Apply.



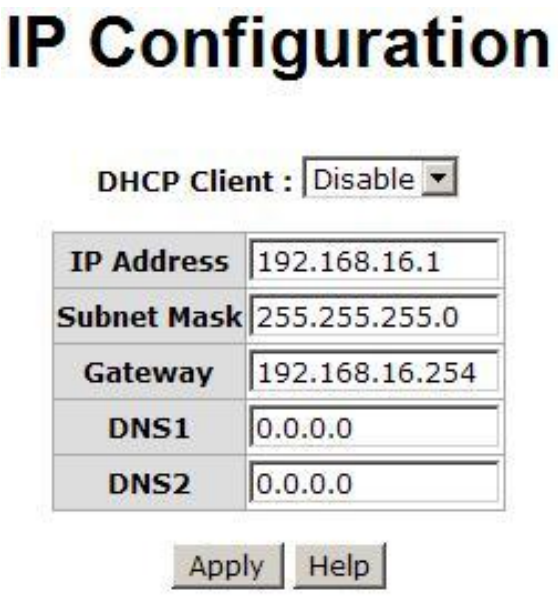
System information interface

6.5 IP Configuration

The switch is a network device which needs to be assigned an IP address for being identified on the network. Users have to decide a means of assigning IP address to the switch.

- **DHCP Client:** Enable or disable the DHCP client function. When DHCP client function is enabled, the switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks **Apply**, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.
- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabled, this switch is configured as a DHCP client. The network DHCP server will assign the IP address to the switch and display it in this column. The default IP is 192.168.16.1 or the user has to assign an IP address manually when DHCP Client is disabled.
- **Subnet Mask:** Assign the subnet mask to the IP address. If DHCP client function is disabled, the user has to assign the subnet mask in this column field.
- **Gateway:** Assign the network gateway for the switch. If DHCP client function is disabled, the user has to assign the gateway in this column field. The default gateway is 192.168.16.254.
- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- And then, click

.



IP configuration interface

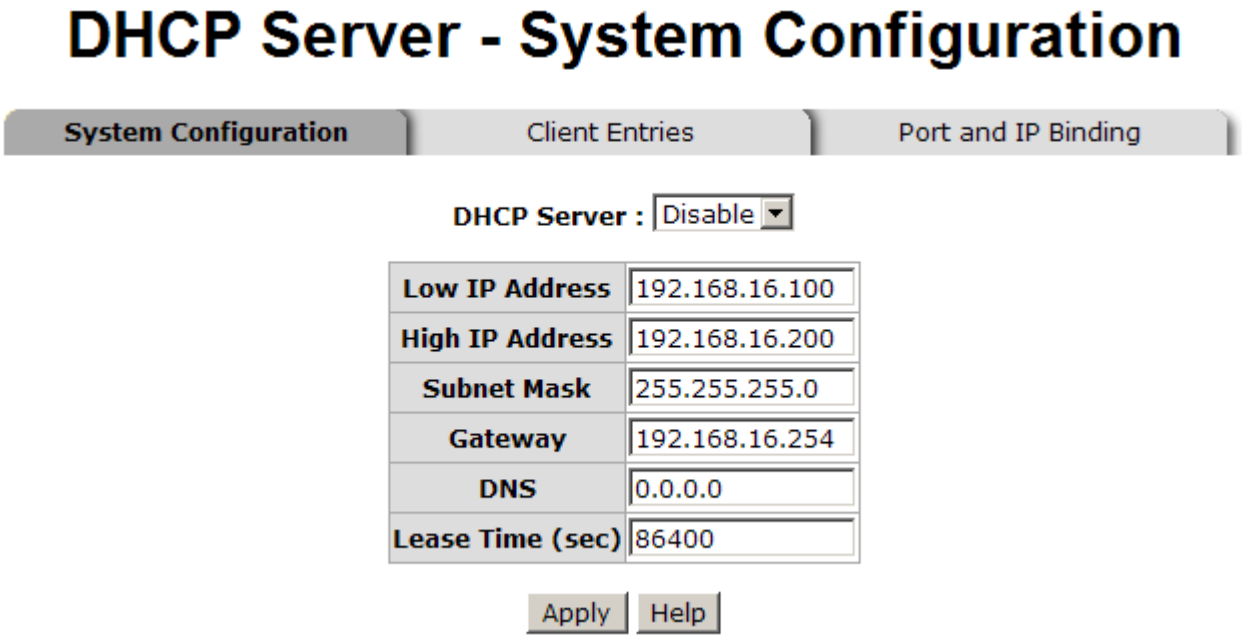
6.6 DHCP Server

DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

The system provides the DHCP server function. Having enabled the DHCP server function, the switch system will be configured as a DHCP server.

6.6.1 System configuration

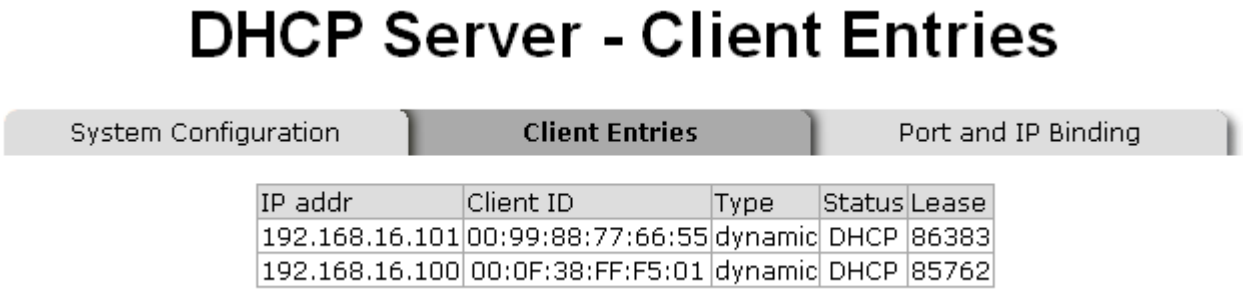
- **DHCP Server:** Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network.
- **Low IP Address:** Type in an IP address. Low IP address is the beginning of the dynamic IP range. For example, dynamic IP is in the range between 192.168.16.100 ~ 192.168.16.200. In contrast, 192.168.16.100 is the Low IP address.
- **High IP Address:** Type in an IP address. High IP address is the end of the dynamic IP range. For example, dynamic IP is in the range between 192.168.16.100 ~ 192.168.16.200. In contrast, 192.168.16.200 is the High IP address.
- **Subnet Mask:** Type in the subnet mask of the IP configuration.
- **Gateway:** Type in the IP address of the gateway in your network.
- **DNS:** Type in the Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
- And then, click Apply.



DHCP Server Configuration interface

6.6.2 Client Entries

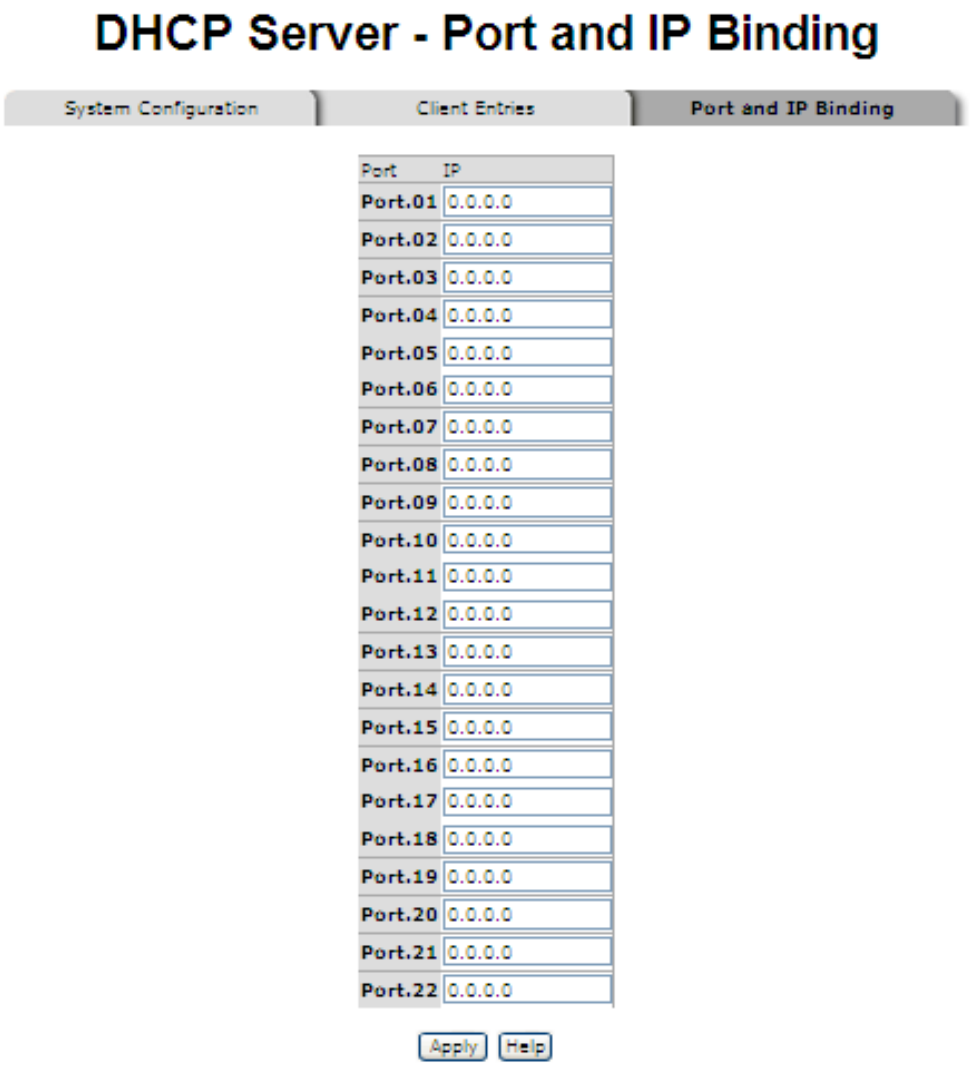
When the DHCP server function is enabled, the system will collect the DHCP client information including the assigned IP address, the MAC address of the client device, the IP assigning type, status and lease time.



DHCP Client Entries interface

6.6.3 Port and IP Bindings

Assign the dynamic IP address bound with the port to the connected client. The user is allowed to fill each port column with one particular IP address. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address bound with the port.



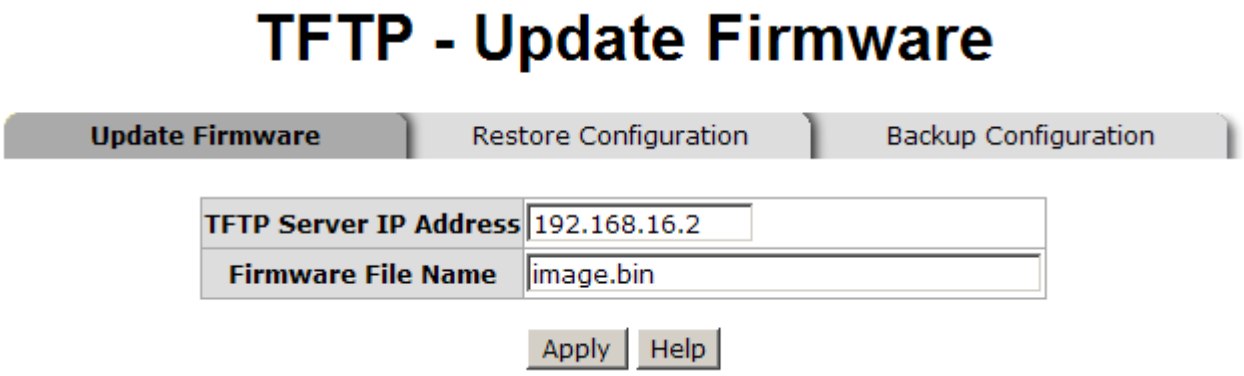
Port and IP Bindings interface

6.7 TFTP

It provides the functions allowing the user to update the switch firmware via the Trivial File Transfer Protocol (TFTP) server. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

6.7.1 Update Firmware

- **TFTP Server IP Address:** Type in your TFTP server IP.
- **Firmware File Name:** Type in the name of the firmware image file to be updated.
- Click Apply.

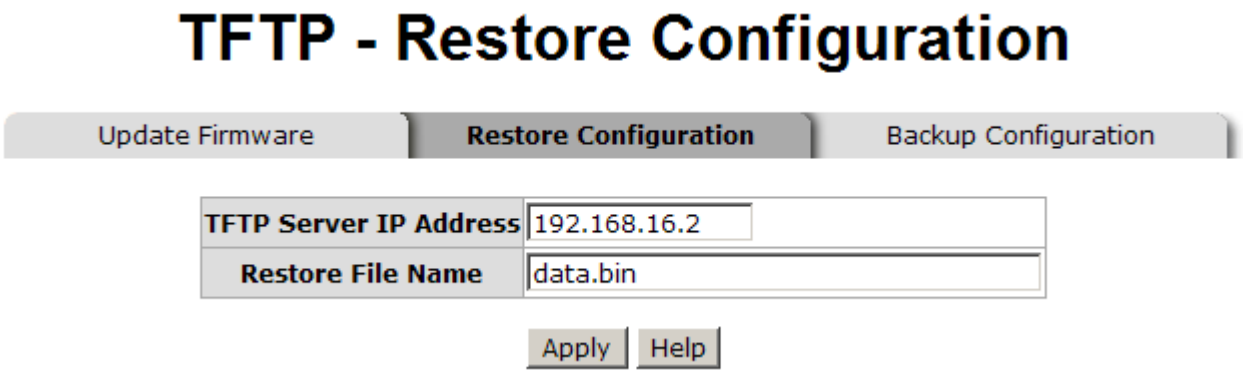


Update Firmware interface

6.7.2 Restore Configuration

You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first and the switch will download back the flash image.

- **TFTP Server IP Address:** Type in the TFTP server IP.
- **Restore File Name:** Type in the correct file name for restoring.
- Click Apply.

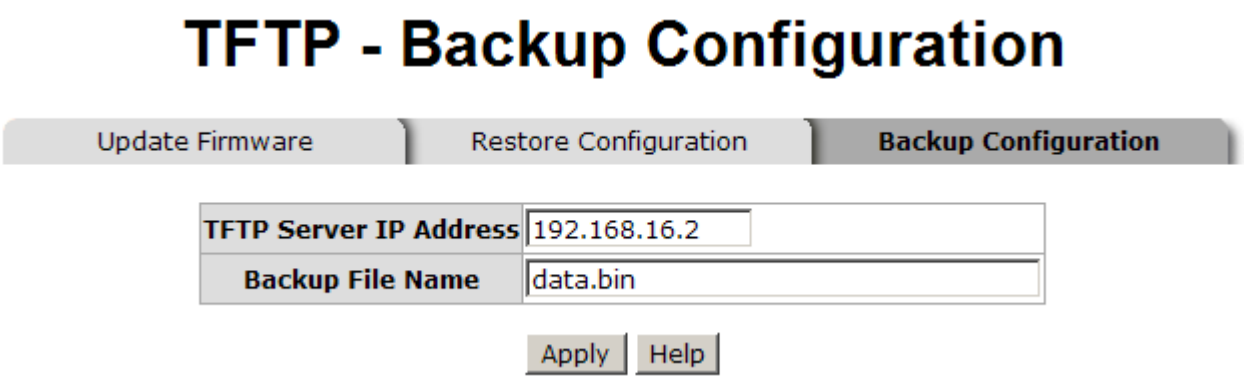


Restore Configuration interface

6.7.3 Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you to avoid wasting time on configuring the settings by backing up the configuration.

- **TFTP Server IP Address:** Type in the TFTP server IP.
- **Backup File Name:** Type in the file name.
- Click Apply.



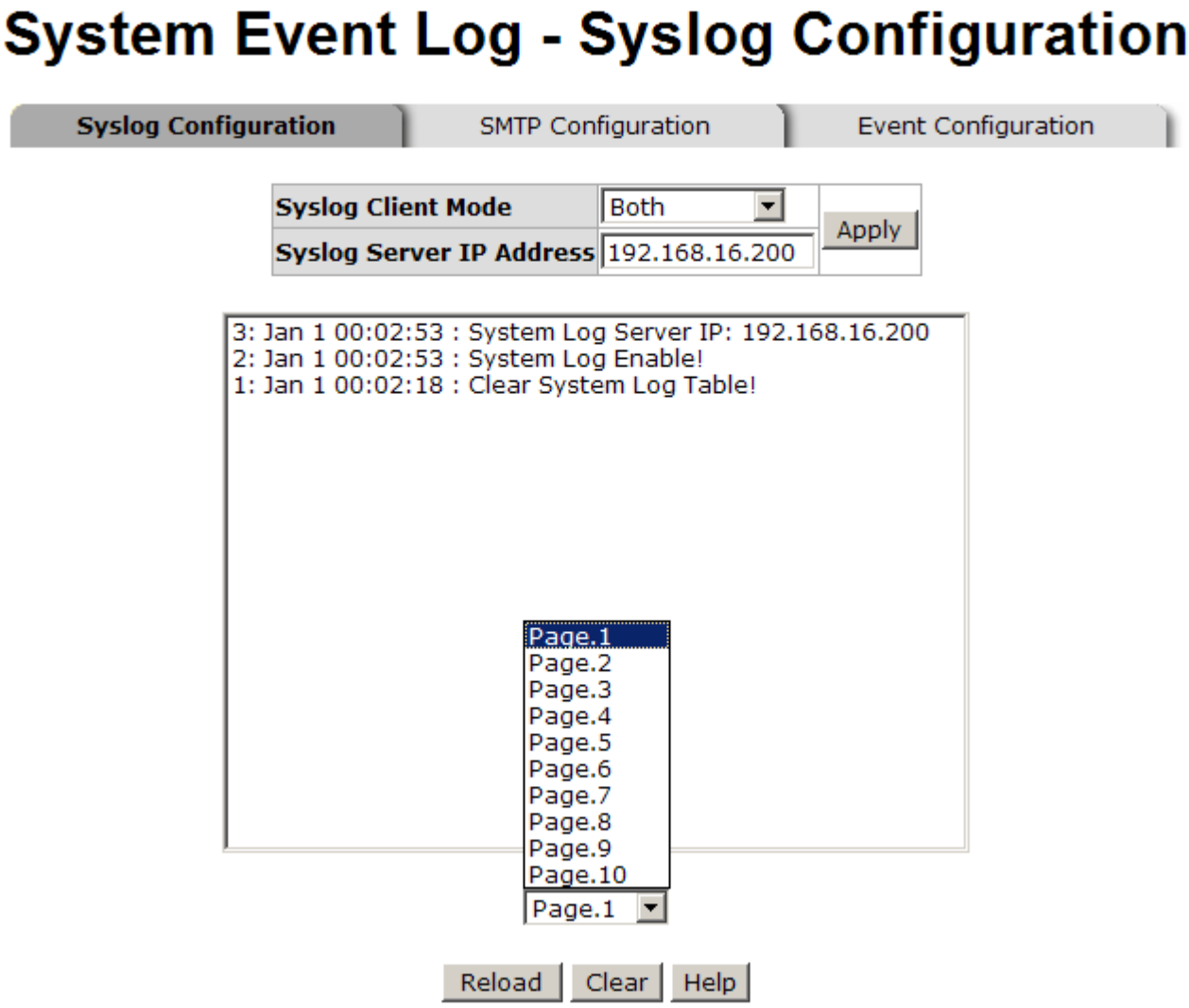
Backup Configuration interface

6.8 System Event Log

This page allows the user to decide whether to send the system event log, and select the mode which the system event log will be sent to client only, server only, or both client and server. What kind of event log will be issued to the client/server depends on the selection on the **Event Configuration** tab. There are five types of event—Device Cold Start, Device Warm Start, Authentication Failure, X-Ring Topology Change, and Port Event—available to be issued as the event log.

6.8.1 Syslog Configuration

- **Syslog Client Mode:** Select the system log mode—**Client Only**, **Server Only**, or **Both**. 'Client Only' means the system event log will only be sent to this interface of the switch, but on the other hand 'Server Only' means the system log will only be sent to the remote system log server with its IP assigned. If the mode is set in 'Both', the system event log will be sent to the remote server and this interface.
- **System Log Server IP Address:** When the 'Syslog Mode' item is set as Server Only/Both, the user has to assign the system log server IP address to which the log will be sent.
- Click Reload to refresh the event log displaying area.
- Click Clear to clear all the current event logs.
- Make sure the selected mode is correct, and click Apply to have the setting take effect.

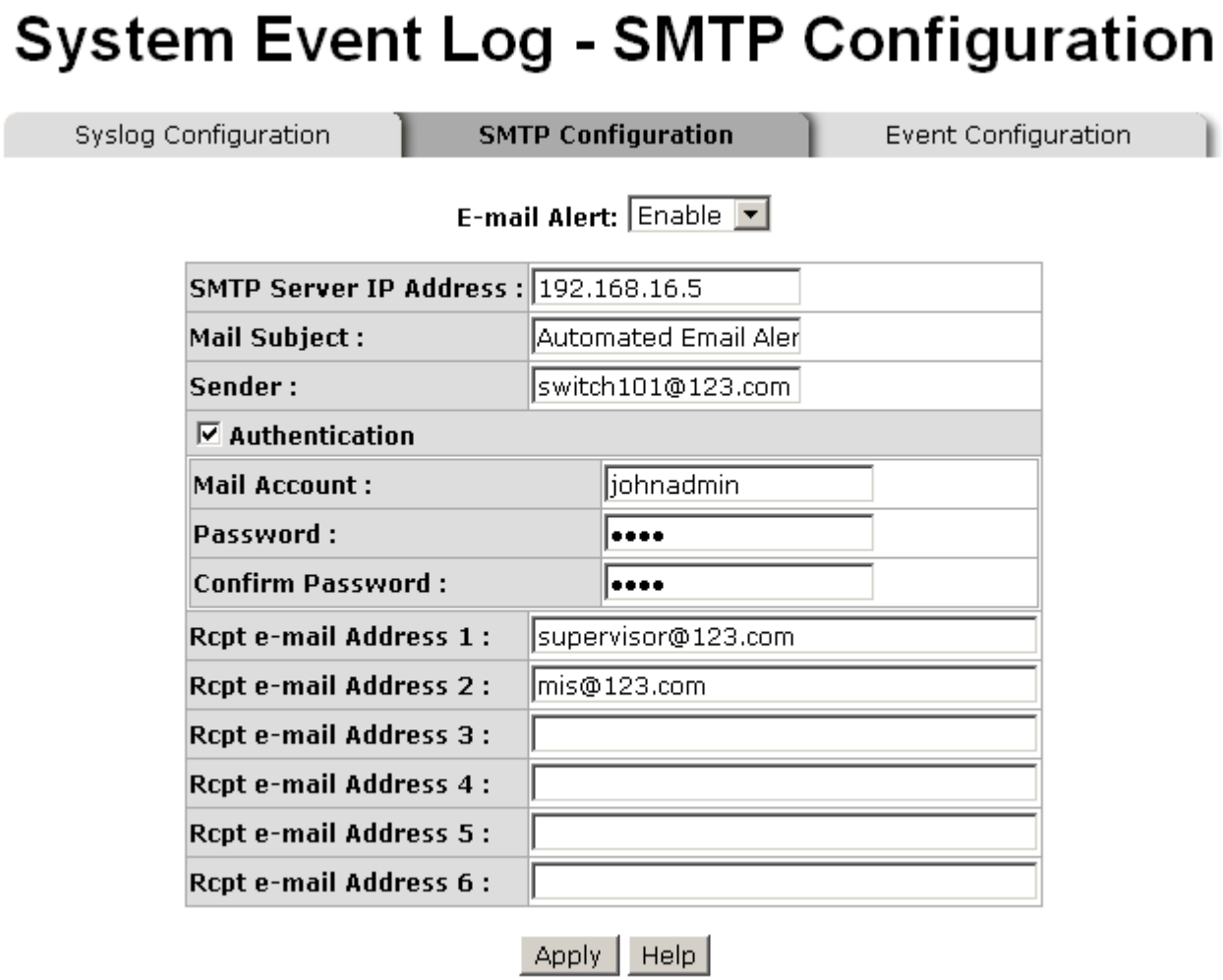


Syslog Configuration interface

6.8.2 System Event Log—SMTP Configuration

Simple Mail Transfer Protocol (SMTP) is the standard for email transmissions across the network. You can configure the SMTP server IP, mail subject, sender, mail account, password, and the recipient email addresses which the e-mail alert will send to. There are also five types of event—Device Cold Start, Device Warm Start, Authentication Failure, X-Ring Topology Change, and Port Event—available to be issued as the e-mail alert. Besides, this function provides the authentication mechanism including an authentication step through which the client effectively logs in to the SMTP server during the process of sending e-mail alert.

- **Email Alert:** With this function being enabled, the user is allowed to configure the detail settings for sending the e-mail alert to the SMTP server when the events occur.
- **SMTP Server IP:** Assign the mail server IP address (when **Email Alert** is enabled, this function will then be available).
- **Mail Subject:** The subject of the mail. Users can modify the string.
- **Sender:** Type in an alias of the switch in complete email address format, e.g. switch101@123.com, to identify where the e-mail alert comes from.
- **Authentication:** Having ticked this checkbox, the mail account, password and confirm password column fields will then show up. Configure the email account and password for authentication when this switch logs in to the SMTP server.
- **Mail Account:** Set up the email account, e.g. johnadmin, to receive the email alert. It must be an existing email account on the mail server.
- **Password:** Type in the password for the email account.
- **Confirm Password:** Reconfirm the password.
- **Rcpt e-mail Address 1 ~ 6:** You can also fill each of the column fields with up to 6 e-mail accounts to receive the email alert.
- Click Apply to have the configuration take effect.



SMTP Configuration interface

6.8.3 System Event Log—Event Configuration

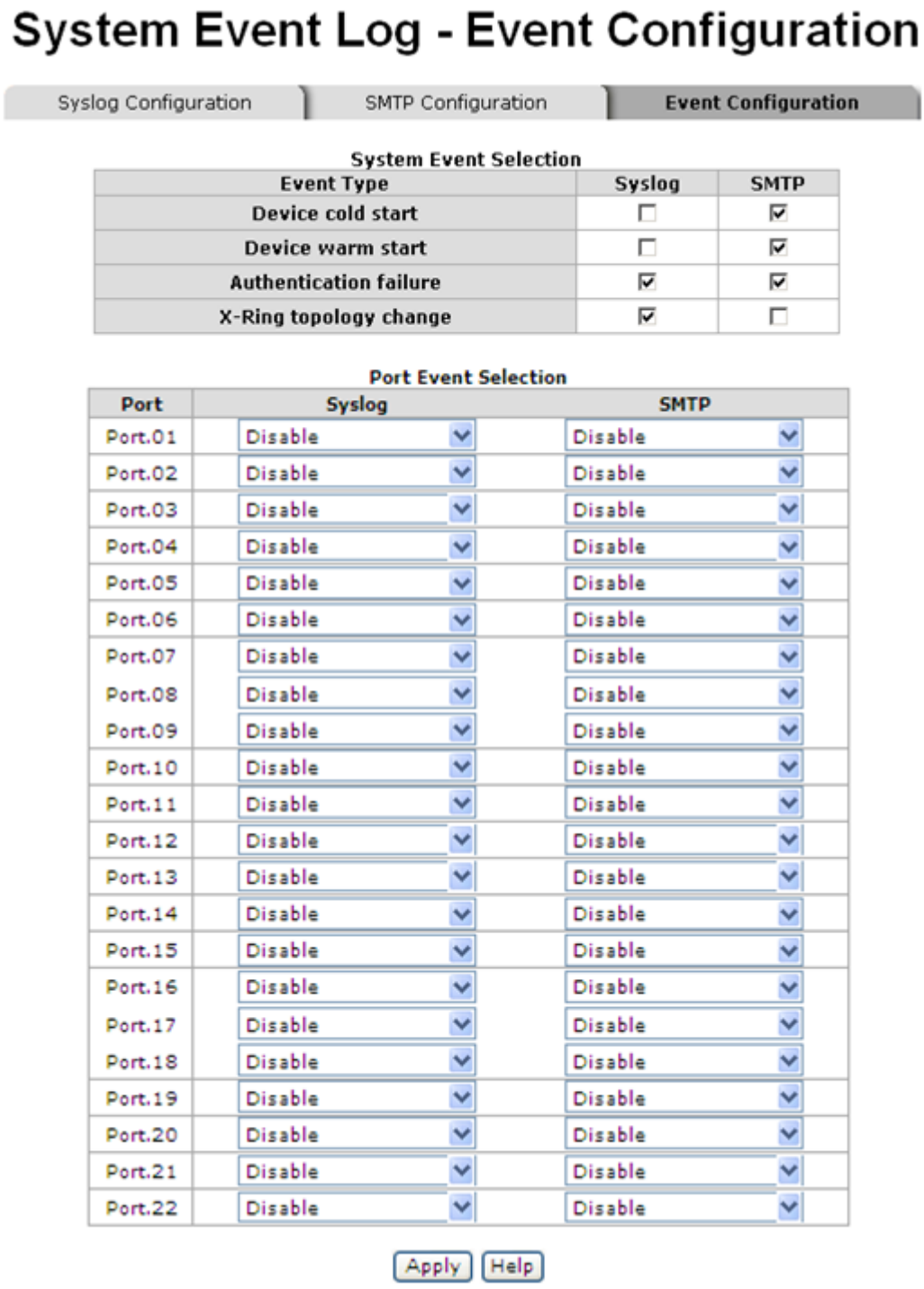
Having ticked the **Syslog**/**SMTP** checkboxes, the event log/email alert will be sent to the system log server and the SMTP server respectively. Also, Port event log/alert (link up, link down, and both) can be sent to the system log server/SMTP server respectively by setting the trigger condition.

- **System event selection:** There are 4 event types—Device Cold Start, Device Warm Start, Authentication Failure, and X-ring Topology Change. The checkboxes are not available for ticking unless the **Syslog Client Mode** on the Syslog Configuration tab and the **E-mail Alert** on the SMTP Configuration tab are enabled first.
  - **Device cold start:** When the device executes cold start action, the system will issue the event log/email alert to the system log/SMTP server respectively.
  - **Device warm start:** When the device executes warm start, the system will issue the event log/email alert to the system log/SMTP server respectively.
  - **Authentication Failure:** When the SNMP authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.
  - **X-ring topology change:** When the X-ring topology has changed, the system will issue the event log/email alert to the system log/SMTP server respectively.

- **Port event selection:** Also, before the drop-down menu items are available, the **Syslog Client Mode** selection item on the Syslog Configuration tab and the **E-mail Alert** selection item on the SMTP Configuration tab must be enabled first. Those drop-down menu items have 3 selections—**Link UP**, **Link Down**, and **Link UP & Link Down**. Disable means no event will be sent to the system log/SMTP server.
  - **Link UP:** The system will only issue a log message when the link-up event of the port occurs.
  - **Link Down:** The system will only issue a log message when the link-down

event of port occurs.

- **Link UP & Link Down:** The system will issue a log message at the time when port connection is link-up and link-down.

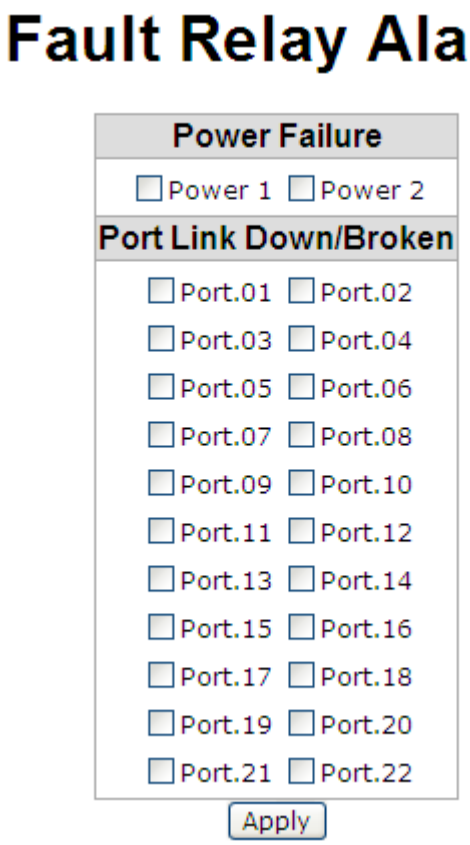


Event Configuration interface

6.9 Fault Relay Alarm

The Fault Relay Alarm function provides the Power Failure and Port Link Down/Broken detection. With both power input 1 and power input 2 installed and the checkboxes of power 1/power 2 ticked, the P-Fail LED indicator will then be possible to light up when any one of the power failures occurs. As for the Port Link Down/Broken detection, the Fail LED indicator will light up when the port failure occurs; certainly the check box beside the port must be ticked first. Please refer to the segment of '**Wiring the P-Fail Alarm Contact**' for the failure detection.

- **Power Failure:** Tick the check box to enable the function of lighting up the **P-Fail** LED on the panel when power fails.
- **Port Link Down/Broken:** Tick the check box to enable the function of lighting up **P-Fail** LED on the panel when Ports' states are link down or broken.



Fault Relay Alarm interface

6.10 SNTP Configuration

SNTP (Simple Network Time Protocol) is a simplified version of NTP which is an Internet protocol used to synchronize the clocks of computers to some time reference. Because time usually just advances, the time on different node stations will be different. With the communicating programs running on those devices, it would cause time to jump forward and back, a non-desirable effect. Therefore, the switch provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and the local clock in each participating subnet peer.

Daylight saving time (DST) is the convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

- **SNTP Client:** Enable/disable SNTP function to get the time from the SNTP server.
- **Daylight Saving Time:** This is used as a control switch to enable/disable daylight saving period and daylight saving offset. Users can configure Daylight Saving Period and Daylight Saving Offset in a certain period time and offset time while there is no need to enable daylight saving function. Afterwards, users can just set this item as enable without assign Daylight Saving Period and Daylight Saving Offset again.
- **UTC Timezone:** Universal Time, Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am

AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm

WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

- **SNTP Sever URL:** Set the SNTP server IP address. You can assign a local network time server IP address or an internet time server IP address.
- **Switch Timer:** When the switch has successfully connected to the SNTP server whose IP address was assigned in the column field of SNTP Server URL, the current coordinated time is displayed here.
- **Daylight Saving Period:** Set up the Daylight Saving beginning date/time and Daylight Saving ending date/time. Please key in the value in the format of 'YYYYMMDD' and 'HH:MM' (leave a space between 'YYYYMMDD' and 'HH:MM').
  - **YYYYMMDD:** an eight-digit year/month/day specification.
  - **HH:MM:** a five-digit (including a colon mark) hour/minute specification.

  For example, key in '20070701 02:00' and '20071104 02:04' in the two column fields respectively to represent that DST begins at 2:00 a.m. on March 11, 2007 and ends at 2:00 a.m. on November 4, 2007.
- **Daylight Saving Offset (mins):** For non-US and European countries, specify the amount of time for day light savings. Please key in the valid figure in the range of minute between 0 and 720, which means you can set the offset up to 12 hours.

- Click Apply to have the configuration take effect.

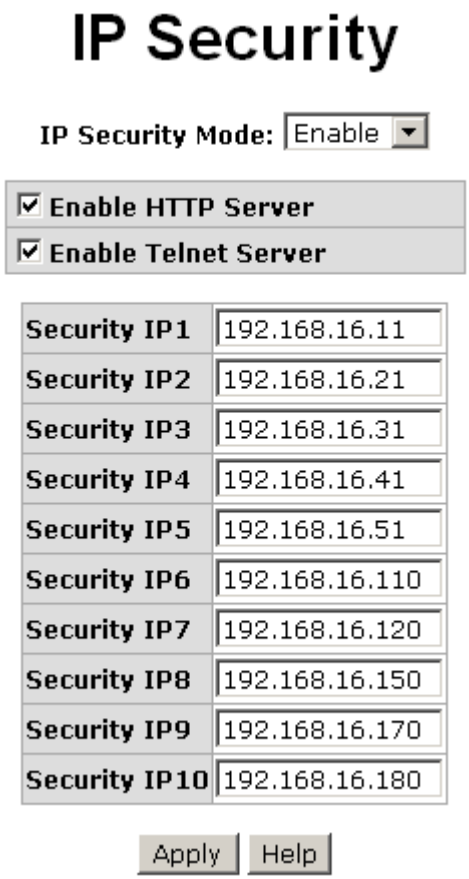
SNTP Configuration interface

6.11 IP Security

IP security function allows the user to assign 10 specific IP addresses that have permission to manage the switch through the http and telnet services for the securing switch management. The purpose of giving the limited IP addresses permission is to allow only the authorized personnel/device can do the management task on the switch.

- **IP Security Mode:** Having set this selection item in the **Enable** mode, the **Enable HTTP Server**, **Enable Telnet Server** checkboxes and the ten security IP column fields will then be available. If not, those items will appear in grey.
- **Enable HTTP Server:** Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via HTTP service.
- **Enable Telnet Server:** Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via telnet service.
- **Security IP 1 ~ 10:** The system allows the user to assign up to 10 specific IP addresses for access security. Only these 10 IP addresses can access and manage the switch through the HTTP/Telnet service once **IP Security Mode** is enabled.
- And then, click Apply to have the configuration take effect.

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.



IP Security interface

6.12 User Authentication

Change web management login user name and password for the management security issue.

- **User name:** Type in the new user name (The default is ‘root’)
- **Password:** Type in the new password (The default is ‘root’)
- **Confirm password:** Re-type the new password
- And then, click Apply

User Authentication interface

6.13 Advanced Configuration

This page enables the user to select the filter packet type including **Flooded Unicast/Multicast Packets**, **Control Packets**, **IP Multicast Packets**, and **Broadcast Packets** for the purpose of limiting the network bandwidth not being occupied by those storm-like packets. All the packet type filtering conditions can be active at the same time. Besides, the user can configure **Broadcast Storm Rate** of this switch to limit the ingress broadcast storm rate.

Flooded Unicast: LAN switches use forwarding tables to direct traffic to specific ports based on the VLAN number and the destination MAC address of the frame. When there is no entry corresponding to the frame's destination MAC address in the incoming VLAN, the unicast frame will be sent to all forwarding ports within the respective VLAN, which causes flooding.

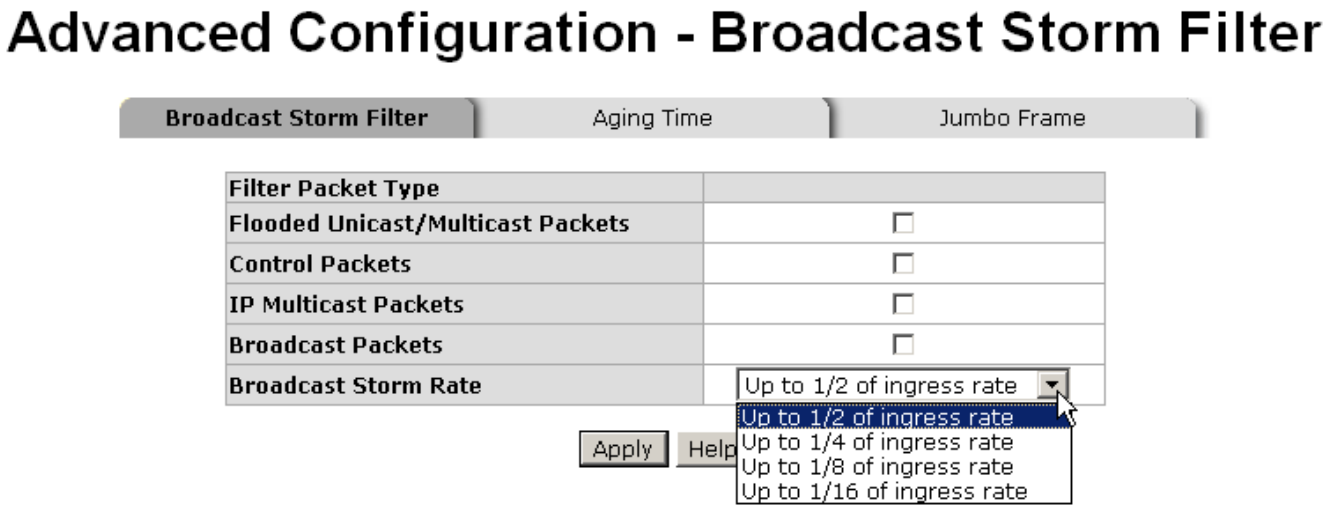
Multicast: Multicast is the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the destinations split.

IP Multicast Packets: An IP Multicast group address is used by sources and the receivers to send and receive packets. Sources use the group address as the IP destination address in their data packets. Receivers use this group address to inform the network that they are interested in receiving packets sent to that group.

6.13.1 Broadcast Storm Filter

- **Flooded Unicast/Multicast Packets:** When this checkbox is ticked, the switch will filter the flooded Unicast/Multicast packets in accordance with the filter rate set in the **Broadcast Storm Rate** selection item.
- **Control Packets:** Having ticked this checkbox, the switch will enable the filter of control packets including BPDU (RSTP/LACP/GVRP), ARP, EAPOL etc. in accordance with the filter rate set in the **Broadcast Storm Rate** selection item.
- **IP multicast Packets:** Having ticked this checkbox, the switch will filter the IP multicast packets in accordance with the filter rate set in the **Broadcast Storm Rate** selection item.

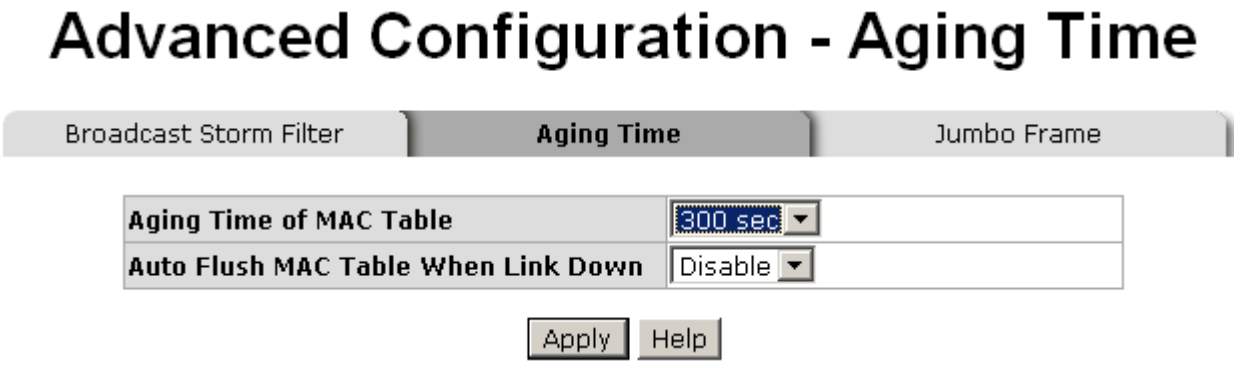
- **Broadcast Packets:** Having ticked this checkbox, the switch will filter the broadcast packets in accordance with the filter rate set in the **Broadcast Storm Rate** selection item.



Broadcast Storm Filter interface

6.13.2 Aging Time

When the MAC address table is full, it won't learn the MAC address any more. Therefore, the aging time function allows users to set aging time in seconds for each record. Once the aging time of the record matches the setting, the record (dynamic MAC address) will be removed from the MAC table. Also, the records will be removed from the MAC table when the particular port links down, which means that every record will be removed if it was learned from that port.

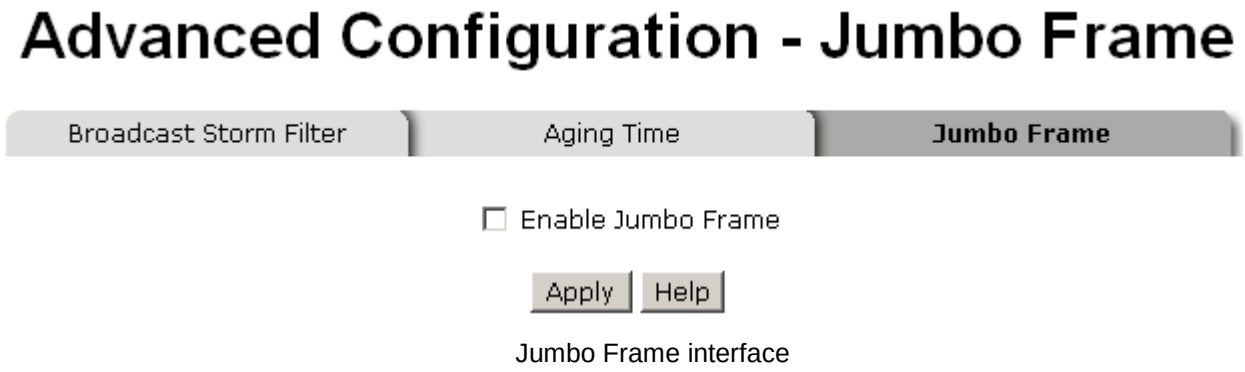


Aging Time interface

- **Aging Time of MAC Table:** Set the aging time as OFF, 150 sec, 300 sec, or 600 sec to remove the record (s) whose property of aging time match this setting.
- **Auto Flush MAC Table When Link Down:** Having enabled this function, the switch will remove the records learned from a particular port when the port links down.
- Click Apply to have the configuration take effect.

6.13.3 Jumbo Frame

Jumbo Frames are Ethernet frames with more than 1522 bytes of payload. Conventionally, jumbo frames can carry up to 9022 bytes of payload. Many, but not all, gigabit Ethernet switches and gigabit Ethernet network interface cards support jumbo frames, but all fast Ethernet switches/network interface cards support only standard-sized frames. It requires hardware and software process for each frame. With the frame size being increased, the same amount of data can be transferred with less effort.

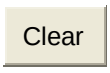


Jumbo Frame interface

- **Enable Jumbo Frame:** Having ticked this checkbox, the switch will allow the jumbo packets (up to 9022 bytes) pass the gigabit port.
- Click Apply to have the configuration take effect.

6.14 Port Statistics

The following chart provides the current statistic information which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

- **Port:** The index column of the ports.
- **Type:** Displays the connection media type of the port.
- **Link:** The status of linking—'**Up**' or '**Down**'.
- **State:** The user can set the state of the port as 'Enable' or 'Disable' via the **Port Control** interface the next function. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of the transmitted good packets via this port.
- **Tx Bad Packet:** The counts of the transmitted bad packets (including undersize [less than 64 bytes], oversize, CRC Align errors, fragments and jabber packets) via this port.
- **Rx Good Packet:** The counts of the received good packets via this port.
- **Rx Bad Packet:** The counts of the received bad packets (including undersize [less than 64 bytes], oversize, CRC Align error, fragments and jabber packets) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- Click  to clean all counts.

Port Statistics

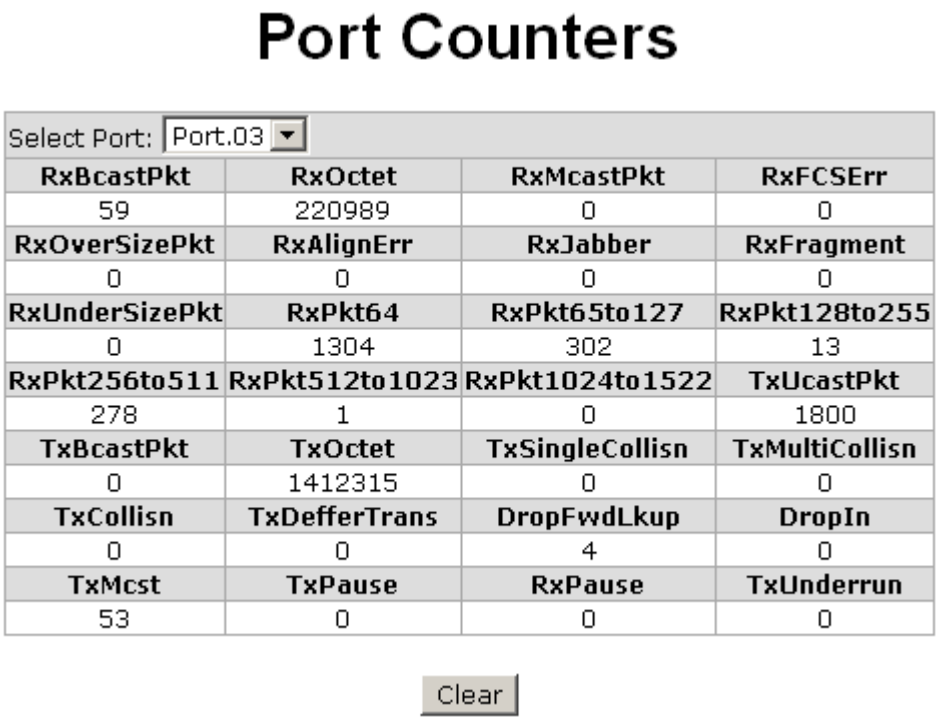
Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.11	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.12	100FX-MM	Down	Enable	0	0	0	0	0	0	0	0	0
Port.13	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.14	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.15	100TX	Up	Enable	736	0	1063	0	0	0	98	253	23
Port.16	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.17	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.18	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.19	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.20	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.21	1000SFP	Down	Enable	0	0	0	0	0	0	0	0	0
Port.22	1000SFP	Down	Enable	0	0	0	0	0	0	0	0	0

Clear Help

Port Statistics interface

6.15 Port Counters

This chart displays the transmitted and received traffic of single port.



- **Select Port:** Pull down the menu bar to select a particular port, and then the counters for the port will be displayed.
- **RxBcastPkt:** The number of good broadcast packets received.
- **RxOctel:** The number of octels of data received (including those in bad packet, excluding framing bits but including FCS octels, excluding RxPausePkt).
- **RxMcastPkt:** The number of good multicast packets received except broadcast packets).
- **RxFCSErr:** The number of packets received that had a bad FCS or RX ER asserted with the proper and integral octels.
- **RxOverSizePkt:** The number of packets received that were longer than Max_Pkt_Len (=1522 bytes) and were otherwise well formed.
- **RxAlignErr:** The number of packets received that had a bad FCS or RX_ER asserted with the proper and non-integral octels.
- **RxJabber:** The number of packets received that were longer than Max_Pkt_Len (=1522 bytes) and had a bad FCS or RX_ER asserted.

- **RxFragment:** The number of packets received that were less than 64 octels long and had a bad FCS or RX_ER asserted.
- **RxUndersizePkt:** The number of packets received that were less than 64 octels long and were otherwise well formed.
- **RxPkt64:** The number of packets received that were 64 octels in length including bad packets but excluding RxPausePkt.
- **RxPkt65to127:** The number of packets received that were between 65 and 127 octels in length (including error packets).
- **RxPkt128to255:** The number of packets received that were between 128 and 255 octels in length (including error packets).
- **RxPkt256to511:** The number of packets received that were between 256 and 511 octels in length (including error packets).
- **RxPkt512to1023:** The number of packets received that were between 511 and 1023 octels in length (including error packets).
- **RxPkt1024to1522:** The number of packets received that were between 1024 and the Max_Pkt_Len (=1522 bytes) octels in length (including error packets).
- **TxUcastPkt:** The number of unicast packet transmitted.
- **TxBcastPkt:** The number of broadcast packet transmitted.
- **TxOctel:** The number of octels transmitted (only for good packets excluding TxPausePkt).
- **TxSingleCollisn:** The number of successfully transmitted packets which transmission is inhibited by exactly one collision.
- **TxMultiCollisn:** The number of successfully transmitted packets which transmission is inhibited by more than one collision.
- **TxCollisn:** The number of collisions on this Ethernet segment.
- **TxDefferTrans:** The number of packets for which the first transmission attempt is delayed because medium is busy.
- **DropFwdLkup:** The number of unicast packets dropped after forwarding table lookup.
- **DropIn:** The number of packets dropped because the input FIFO overrun and the FC violation.
- **TxMcst:** The number of multicast packet transmitted.
- **TxPause:** The number of Pause Packet transmitted.
- **RxPause:** The number of Pause Packet received.

- **TxUnderrun:** The number of packets dropped because the output FIFO underrun.
- Click Clear to reset the figures.

6.16 Port Control

In Port control you can configure the settings of each port to control the connection parameters, and the status of each port is listed beneath.

- **Port:** Use the scroll bar and click on the port number to choose the port to be configured.
- **State:** Current port state. The port can be set to disable or enable mode. If the port state is set as ‘Disable’, it will not receive or transmit any packet.
- **Negotiation:** Auto and Force. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to set the speed and duplex mode manually.
- **Speed:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
- **Duplex:** It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
- **Flow Control:** Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
- **Security:** When the Security selection is set as ‘**On**’, any access from the device which connects to this port will be blocked unless the MAC address of the device is included in the static MAC address table. See the segment of **MAC Address Table—Static MAC Addresses**.
- Click

to have the configuration take effect.

Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.07 Port.08 Port.09 Port.10	Enable	Force	100	Full	Enable	Off

Apply Help

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.02	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.03	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.04	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.05	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.06	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.07	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.08	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.09	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.10	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.11	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.12	N/A	100FX-MM	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.13	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.14	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.15	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Enable	ON	OFF
Port.16	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.17	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.18	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.19	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.20	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.21	N/A	1000SFP	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.22	N/A	1000SFP	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Port Control interface

6.17 Port Trunk

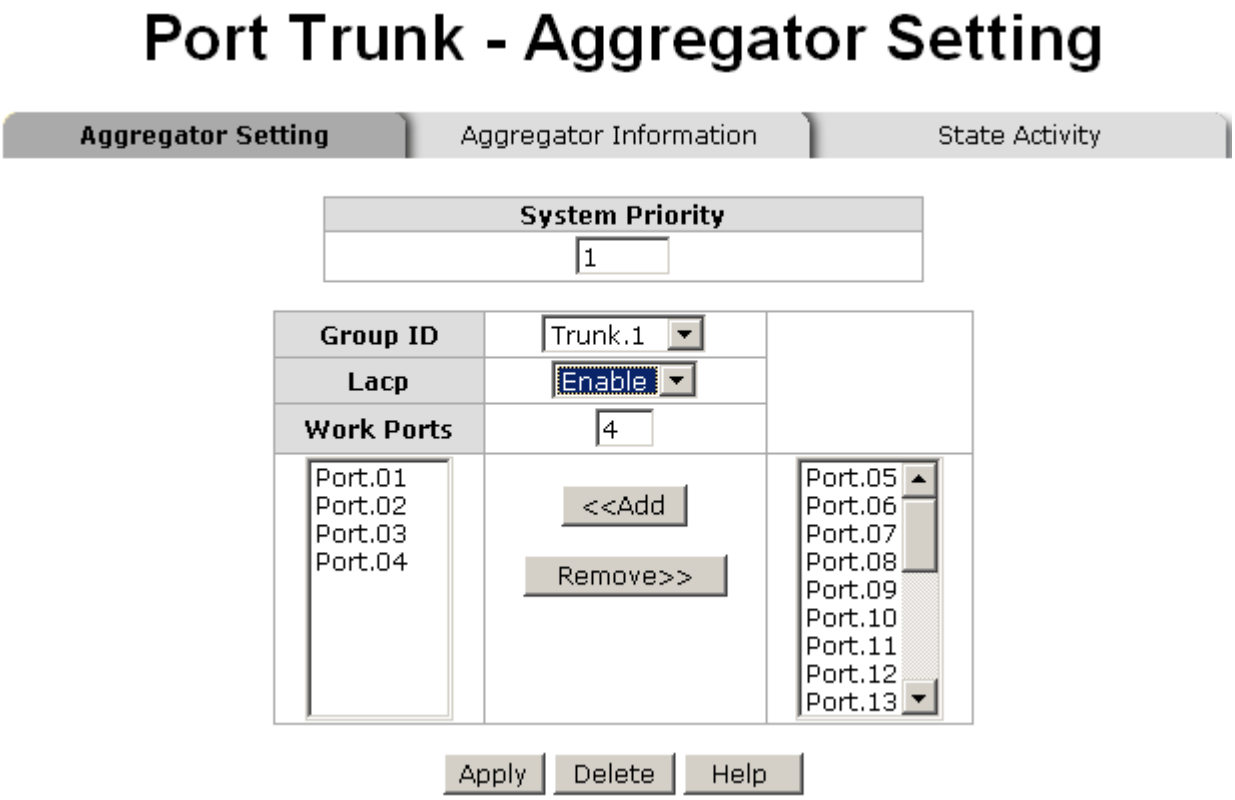
Port trunking is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad to bundle several physical ports together to form a single logical channel. All the ports within the logical channel or so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode.

6.17.1. Aggregator setting

- **System Priority:** A value which is used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.
- **Group ID:** There are 13 trunk groups to be selected. Assign the "**Group ID**" to the trunk group.
- **LACP:** When enabled, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. Please notice that a trunk group, including member ports split between two switches, has to enable the LACP function of the two switches. When disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.
- **Work ports:** This column field allows the user to type in the total number of active port up to four. With **LACP static trunk group**, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a **static trunk group** (non-LACP), the number of work ports must equal the total number of group member ports.
- Select the ports to join the trunk group. The system allows a maximum of four ports to be aggregated in a trunk group. Click and the ports focused in

the right side will be shifted to the left side. To remove unwanted ports, select the ports and click Remove.

- When LACP enabled, you can configure LACP Active/Passive status for each port on the **State Activity** tab.
- Click Apply.
- Use Delete to delete Trunk Group. Select the Group ID and click Delete.

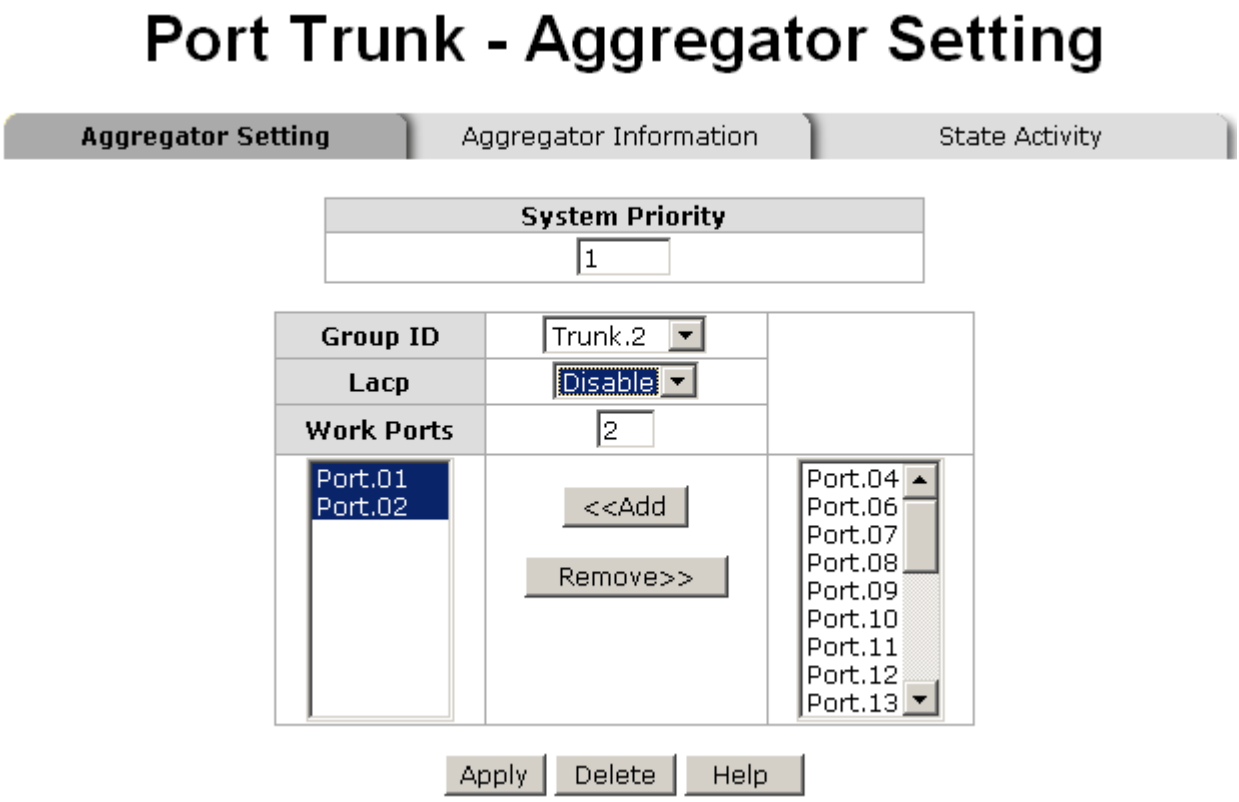


Port Trunk—Aggregator Setting interface (four ports are added to the left field with LACP enabled)

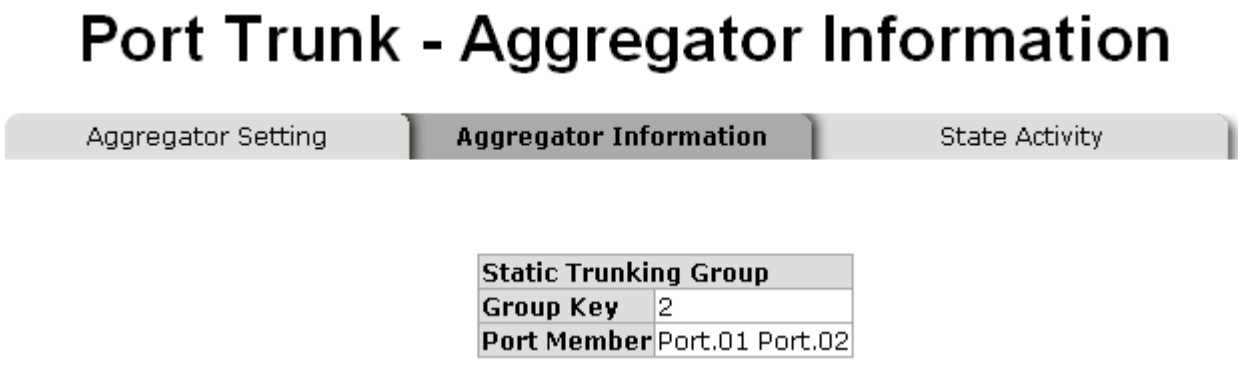
6.17.2. Aggregator Information

LACP disabled

Having set up the aggregator setting with LACP disabled, you will see the local static trunk group information on the tab of **Aggregator Information**.



Assigning 2 ports to a trunk group with LACP disabled



Static Trunking Group information

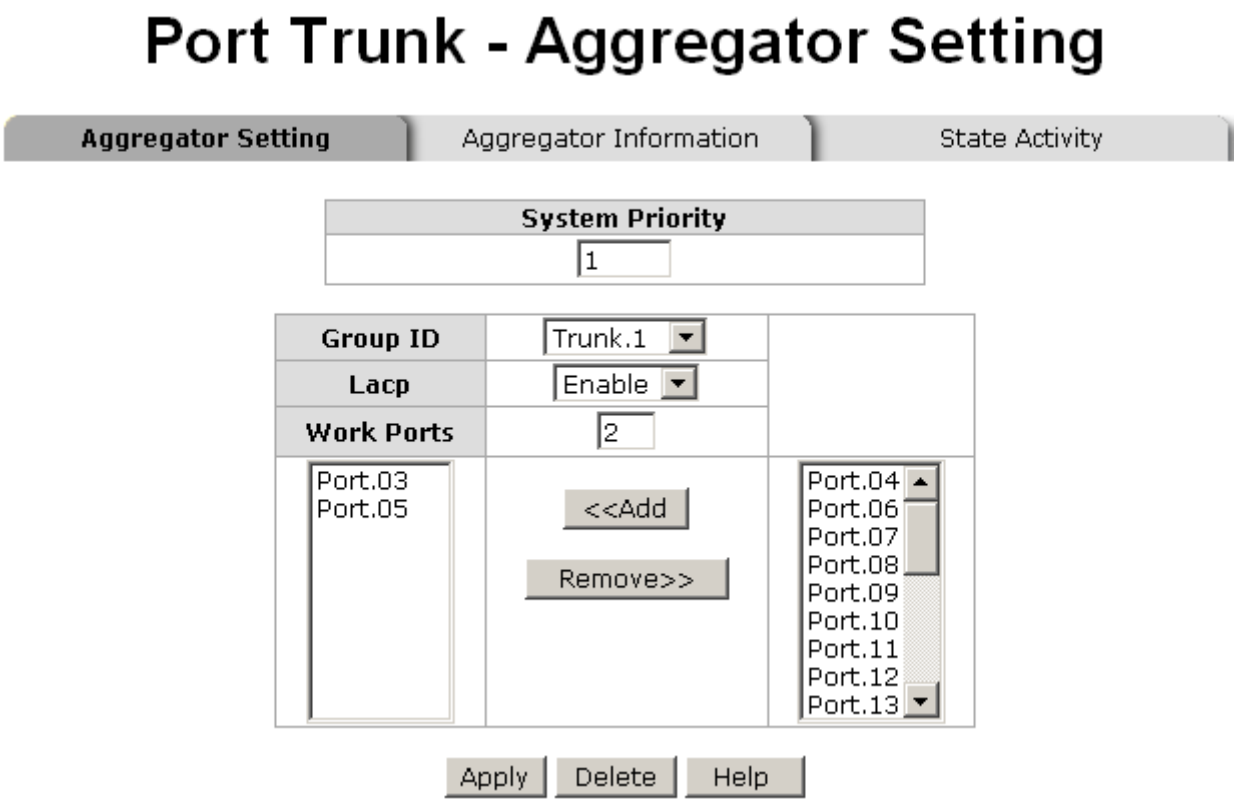
- **Group Key:** This is a read-only column field that displays the trunk group ID.
- **Port Member:** This is a read-only column field that displays the members of this static trunk group.

LACP enabled

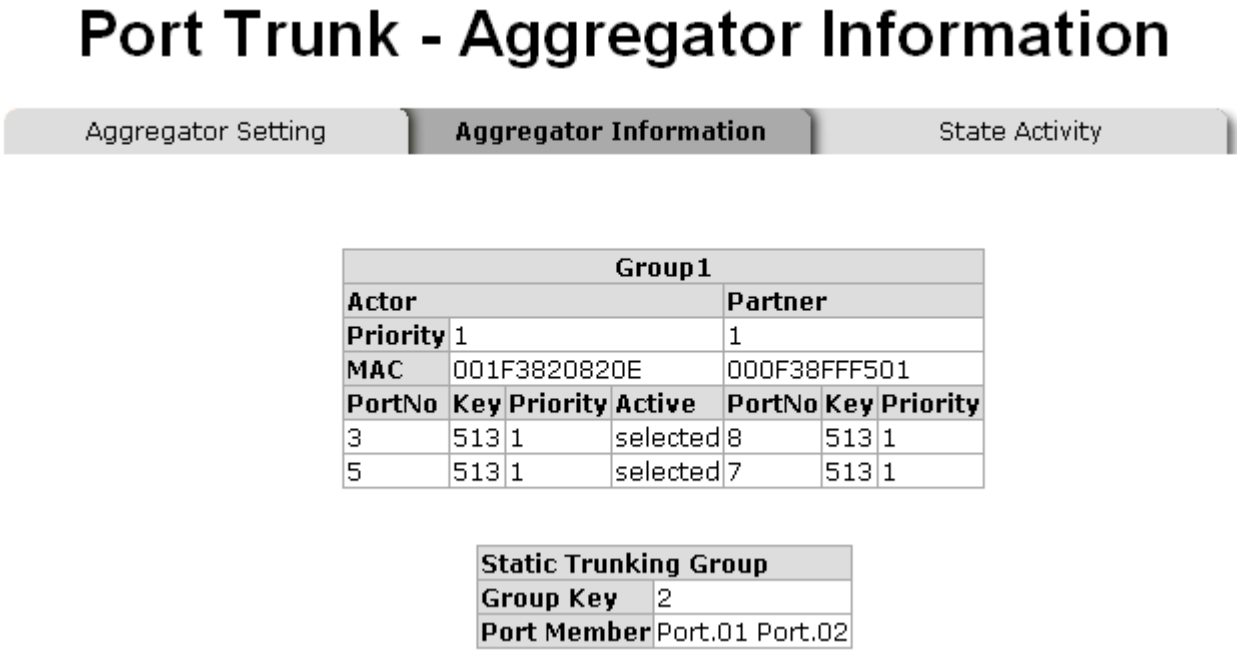
Having set up the aggregator setting with LACP enabled, you will see the trunking group information between two switches on the tab of **Aggregator Information**.

- **Switch 1 configuration**

1. Set **System Priority** of the trunk group. The default is 1.
2. Select a **trunk group ID** by pull down the drop-down menu bar.
3. Enable LACP.
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.



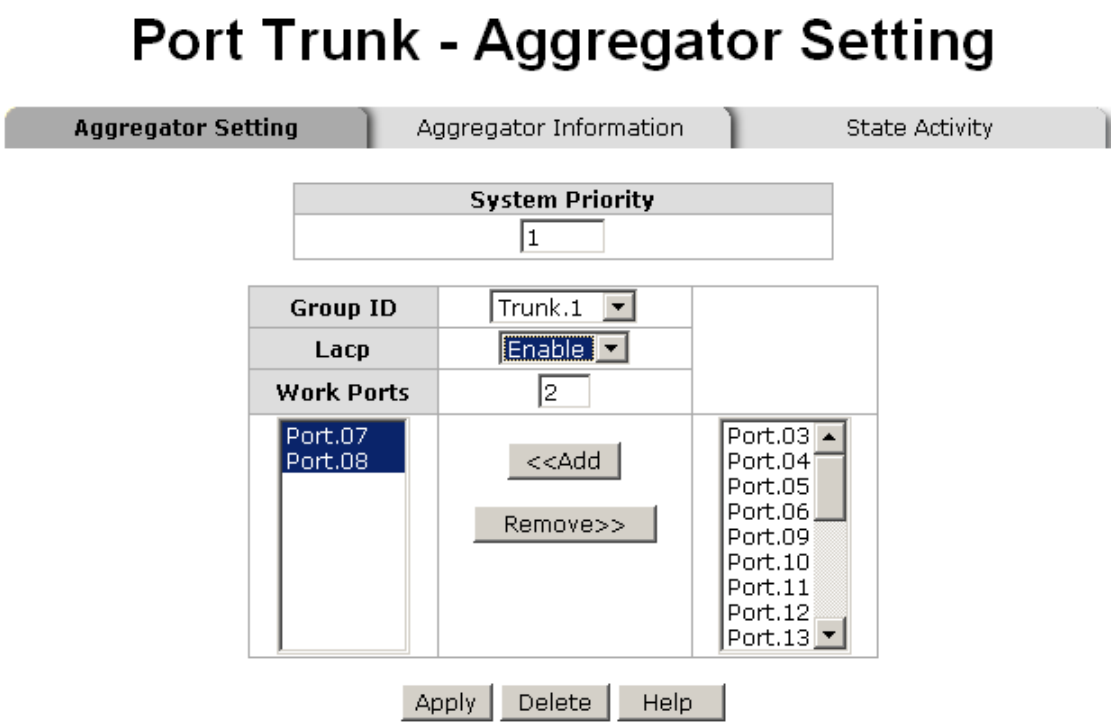
Switch 1 configuration interface



Aggregation Information of Switch 1

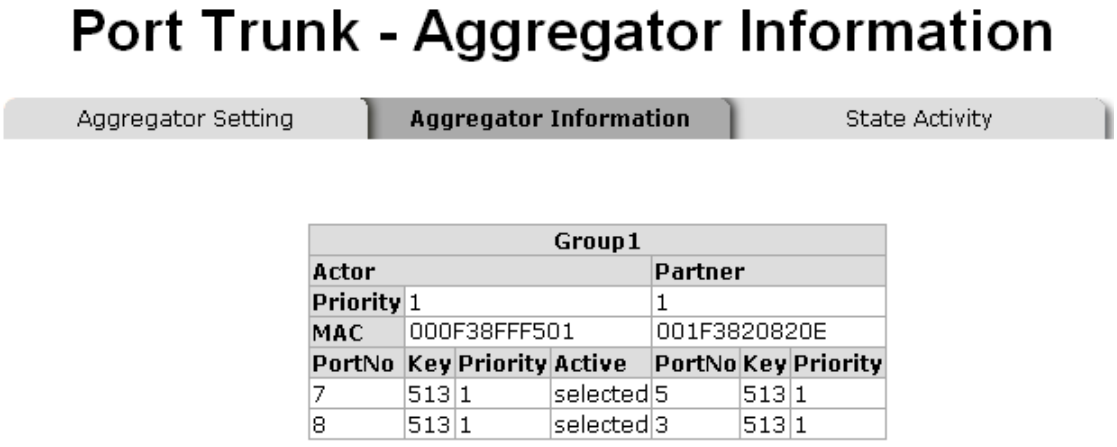
5. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.

■ **Switch 2 configuration**



Switch 2 configuration interface

1. Set **System Priority** of the trunk group. The default is 1.
2. Select a **trunk group ID** by pull down the drop-down menu bar.
3. Enable LACP.
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.



Aggregation Information of Switch 2

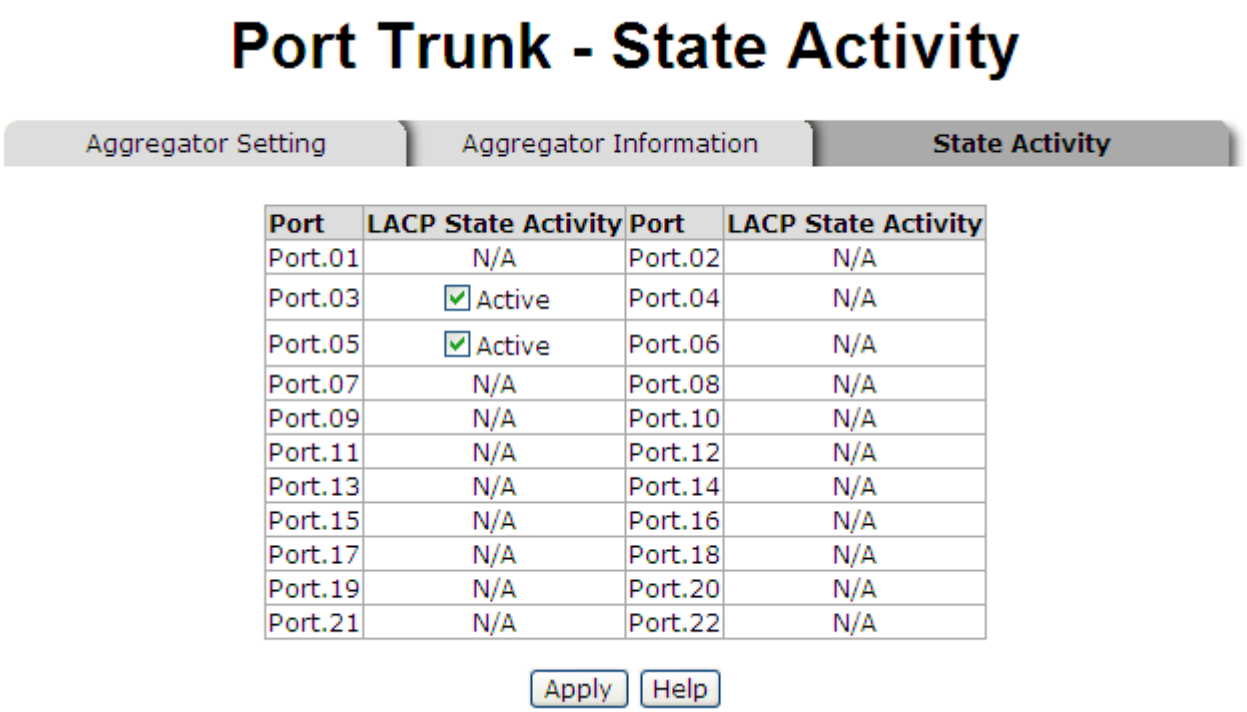
5. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.

6.17.3. State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state label. When you remove the tick mark of the port and click Apply, the port state activity will change to **Passive**.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]	**A link** having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.



State Activity of Switch 1

Port Trunk - State Activity

Aggregator Setting | Aggregator Information | **State Activity**

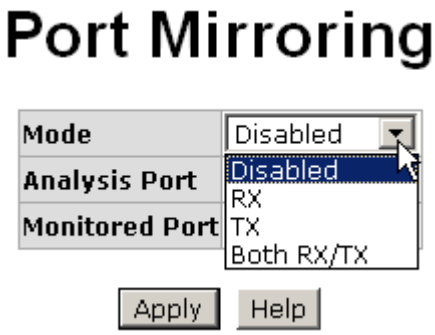
Port	LACP State Activity	Port	LACP State Activity
Port.01	N/A	Port.02	N/A
Port.03	N/A	Port.04	N/A
Port.05	N/A	Port.06	N/A
Port.07	☑ Active	Port.08	☑ Active
Port.09	N/A	Port.10	N/A
Port.11	N/A	Port.12	N/A
Port.13	N/A	Port.14	N/A
Port.15	N/A	Port.16	N/A
Port.17	N/A	Port.18	N/A
Port.19	N/A	Port.20	N/A
Port.21	N/A	Port.22	N/A

Apply Help

State Activity of Switch 2

6.18 Port Mirroring

The Port mirroring is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port, which means traffic goes in or out **Monitored** (source) port will be duplicated into **Analysis** (destination) port.

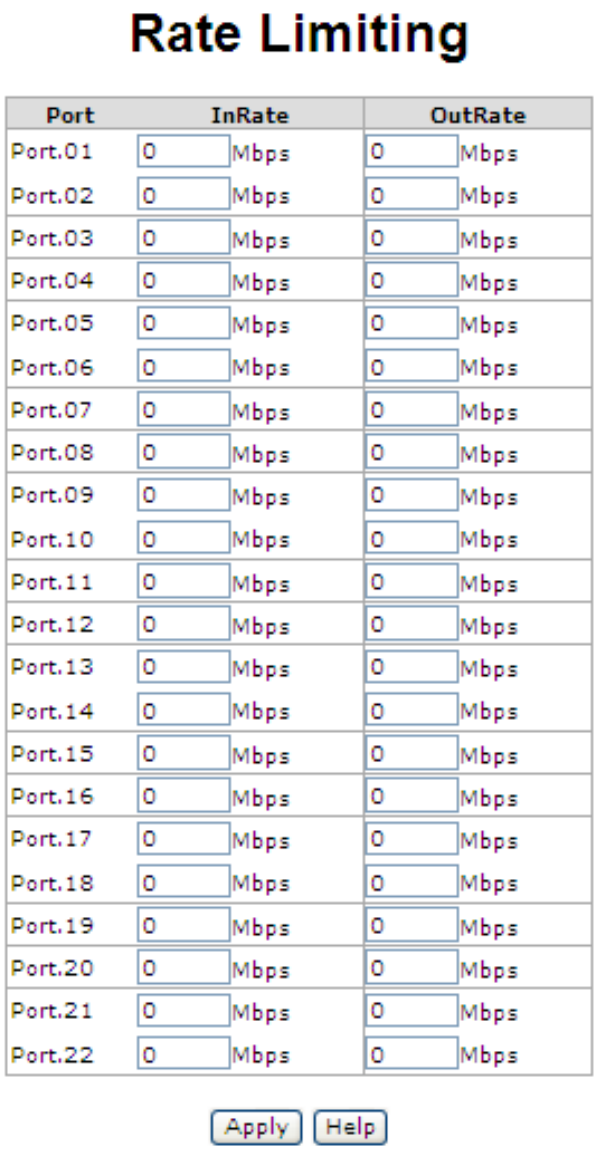


Port Trunk – Port Mirroring interface

- **Mode:** Choose the type of being monitored packets. **RX** means only the received packets of the monitored port will be copied and sent to the analysis port. **TX** means only the transmitted packets of the monitored port will be copied and sent to the analysis port. **Both RX/TX** means both received & transmitted packets of the monitored port will be copied and sent to the analysis port.
- **Analysis Port:** There is only one port can be selected to be the analysis (destination) port for monitoring both RX and TX traffic which come from the source port. Users can connect the analysis port to LAN analyzer or Netxray.
- **Monitored Port:** Choose a port number to be monitored. Only one port can be monitored during the monitoring process.
- And then, click Apply.

6.19 Rate Limiting

All the ports support port ingress and egress rate control. The switch performs the ingress/egress rate by packet counter to meet the specified rate. When the traffic exceeds the limited transfer rate, the packets will be delayed or dropped.


Rate Limiting
Port
InRate
OutRate
Port.01 0 Mbps 0 Mbps
Port.02 0 Mbps 0 Mbps
Port.03 0 Mbps 0 Mbps
Port.04 0 Mbps 0 Mbps
Port.05 0 Mbps 0 Mbps
Port.06 0 Mbps 0 Mbps
Port.07 0 Mbps 0 Mbps
Port.08 0 Mbps 0 Mbps
Port.09 0 Mbps 0 Mbps
Port.10 0 Mbps 0 Mbps
Port.11 0 Mbps 0 Mbps
Port.12 0 Mbps 0 Mbps
Port.13 0 Mbps 0 Mbps
Port.14 0 Mbps 0 Mbps
Port.15 0 Mbps 0 Mbps
Port.16 0 Mbps 0 Mbps
Port.17 0 Mbps 0 Mbps
Port.18 0 Mbps 0 Mbps
Port.19 0 Mbps 0 Mbps
Port.20 0 Mbps 0 Mbps
Port.21 0 Mbps 0 Mbps
Port.22 0 Mbps 0 Mbps
Apply
Help

Rate Limiting interface

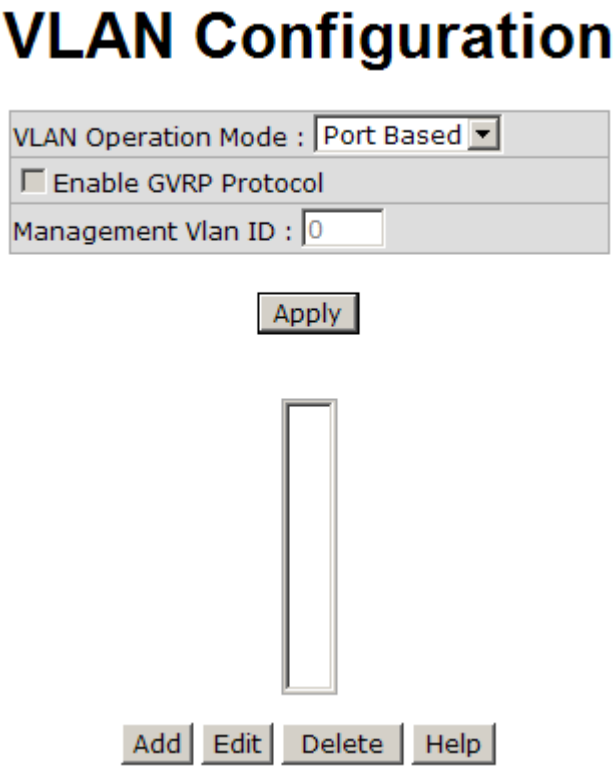
- **Ingress**: Assign the port effective ingress rate (The default value is “0”).
- **Egress**: Assign the port effective egress rate (The default value is “0”).
- And then, click Apply to have the configuration take effect.

6.20 VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN on a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

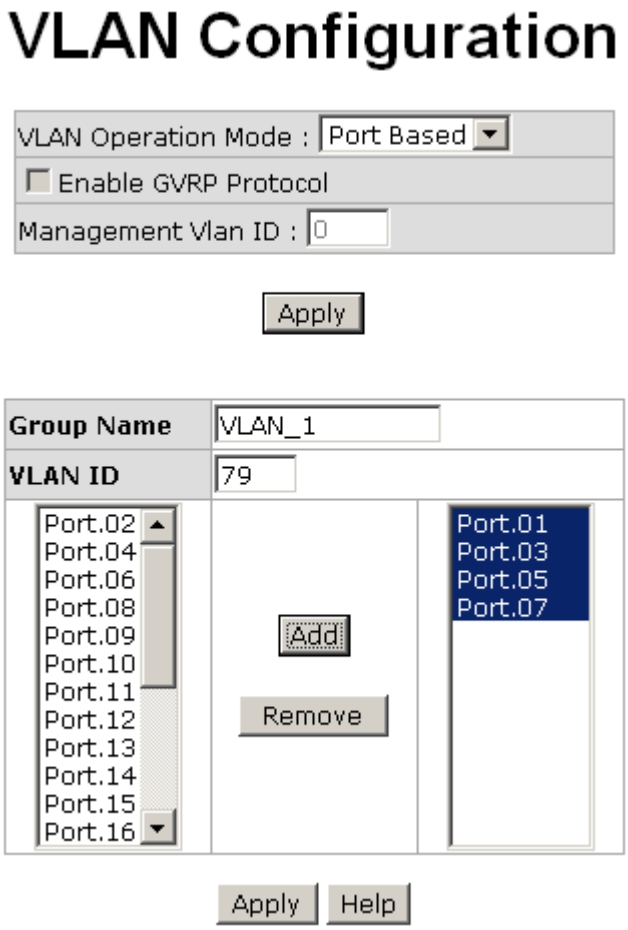
6.20.1. Port-based VLAN

A port-based VLAN basically consists of its members—ports, which means the VLAN is created by grouping the selected ports. This method provides the convenience for users to configure a simple VLAN easily without complicated steps. Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored. The port-based VLAN function allows the user to create separate VLANs to limit the unnecessary packet flooding; however, for the purpose of sharing resource, a single port called a common port can belongs to different VLANs, which all the member devices (ports) in different VLANs have the permission to access the common port while they still cannot communicate with each other in different VLANs.



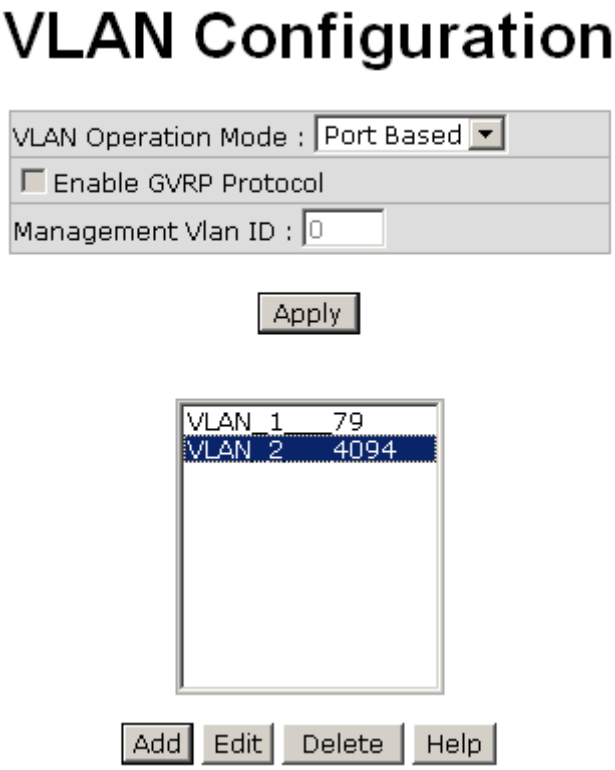
VLAN – Port Based interface

- Pull down the selection item and focus on **Port Based** then press Apply to set the VLAN Operation Mode in **Port Based** mode.
- Click Add to add a new VLAN group (The maximum VLAN groups are up to 64).



VLAN—Port Based Add interface

- Enter the group name and VLAN ID. Add the selected port number into the right field to group these members to be a VLAN group, or remove any of them listed in the right field from the VLAN.
- And then, click Apply to have the configuration take effect.
- You will see the VLAN list displays.



VLAN—Port Based Edit/Delete interface

- Use Delete to delete the VLAN.
- Use Edit to modify group name, VLAN ID, or add/remove the members of the existing VLAN group.

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when switch power off.

6.20.2. 802.1Q VLAN

Virtual Local Area Network (VLAN) can be implemented on the switch to logically create different broadcast domain.

When the 802.1Q VLAN function is enabled, all ports on the switch belong to default VLAN of VID 1, which means they logically are regarded as members of the same broadcast domain. The valid VLAN ID is in the range of number between 1 and 4094. The amount of VLAN groups is up to 256 including default VLAN that cannot be deleted.

Each member port of 802.1Q is on either an Access Link (VLAN-tagged) or a Trunk Link (no VLAN-tagged). All frames on an Access Link carry no VLAN identification. Conversely, all frames on a Trunk Link are VLAN-tagged. Besides, there is the third mode—Hybrid. A Hybrid Link can carry both VLAN-tagged frames and untagged frames. A single port is supposed to belong to one VLAN group, except it is on a Trunk/Hybrid Link.

The technique of 802.1Q tagging inserts a 4-byte tag, including VLAN ID of the destination port—PVID, in the frame. With the combination of Access/Trunk/Hybrid Links, the communication across switches also can make the packet sent through tagged and untagged ports.

802.1Q Configuration

- Pull down the selection item and focus on **802.1Q** then press Apply to set the VLAN Operation Mode in **802.1Q** mode.
- **Enable GVRP Protocol:** GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. For example, having enabled GVRP on two switches, they are able to automatically exchange the information of their VLAN database. Therefore, the user doesn't need to manually configure whether the link is trunk or hybrid, the packets belonging to the same VLAN can communicate across switches. Tick this checkbox to enable GVRP protocol. This checkbox is available while the VLAN Operation Mode is in **802.1Q** mode.
- **Management VLAN ID:** Only when the VLAN members, whose Untagged VID (PVID) equals to the value in this column, will have the permission to access the switch. The default value is '0' that means this limit is not enabled (all members in different VLANs can access this switch).
- Select the port you want to configure.
- **Link Type**: There are 3 types of link type.
  - **Access Link:** A segment which provides the link path for one or more stations to the VLAN-aware device. An Access Port (untagged port), connected to the access link, has an untagged VID (also called PVID). After an untagged frame gets into the access port, the switch will insert a four-byte tag in the frame. The contents of the last 12-bit of the tag is untagged VID. When this frame is sent out through any of the access port of the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are regarded as the same VLAN group members.

Note: Because the access port doesn't have an understanding of tagged frame, the column field of Tagged VID is not available.

- **Trunk Link:** A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, has an understanding of tagged frame, which is used for the communication among VLANs across switches. Which frames of the specified VIDs will be forwarded depends on the values filled in the Tagged VID column field. Please insert a comma between two VIDs.

Note:

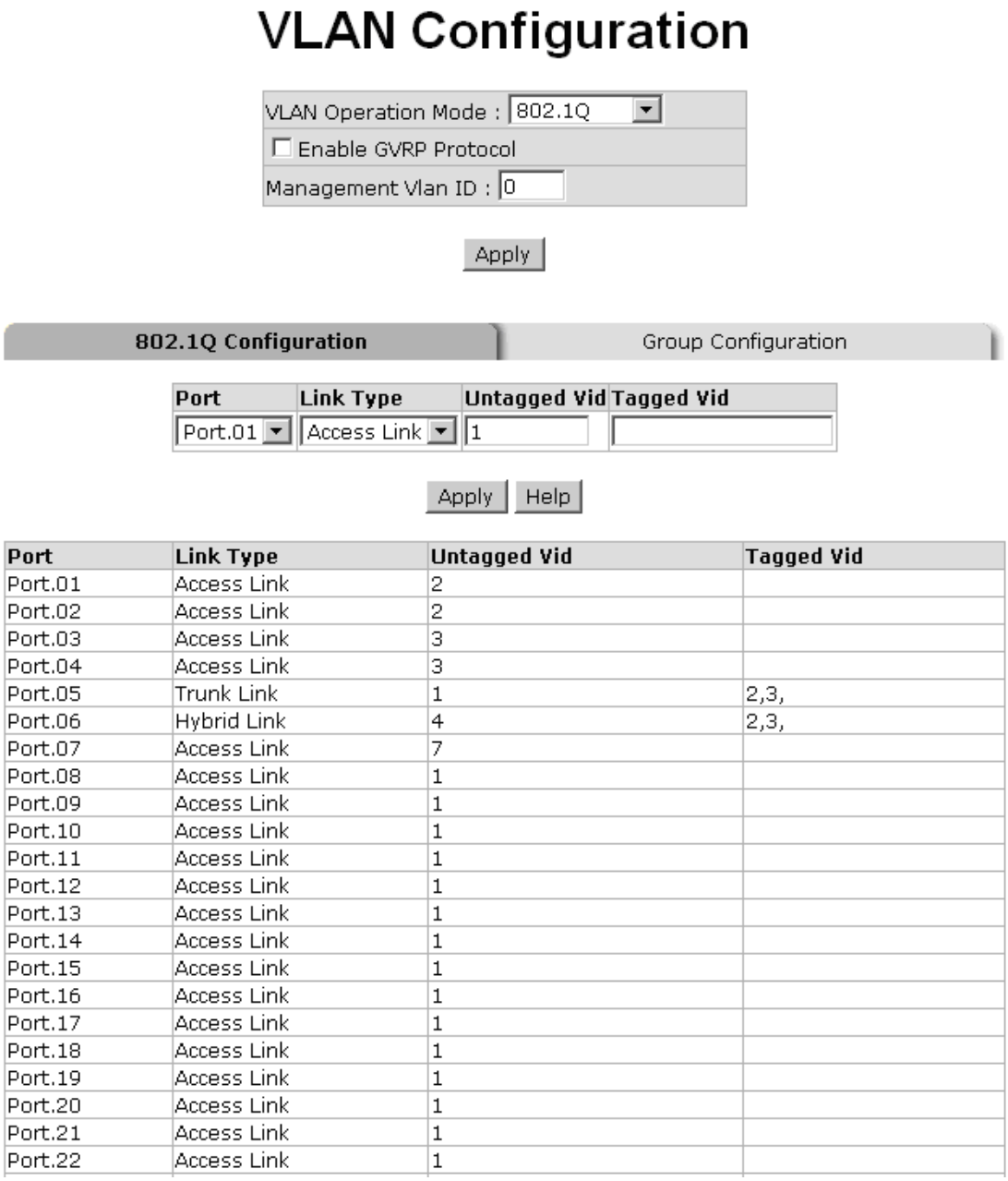
1. *A trunk port doesn't insert tag into an untagged frame, and therefore the untagged VID column field is not available.*
2. *It's not necessary to type '1' in the tagged VID. The trunk port will forward the frames of VLAN 1.*
3. *The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.*

- **Hybrid Link:** A segment which consists of Access and Trunk links. The hybrid port has both the features of access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and it also forwards the specified tagged-frames for the purpose of VLAN communication across switches.

Note:

1. *It's not necessary to type '1' in the tagged VID. The hybrid port will forward the frames of VLAN 1.*
2. *The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.*

- **Untagged VID:** This column field is available when Link Type is set as Access Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- **Tagged VID:** This column field is available when Link Type is set as Trunk Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- Click Apply to have the configuration take effect.
- You can see the link type, untagged VID, and tagged VID information of each port in the table below on the screen.

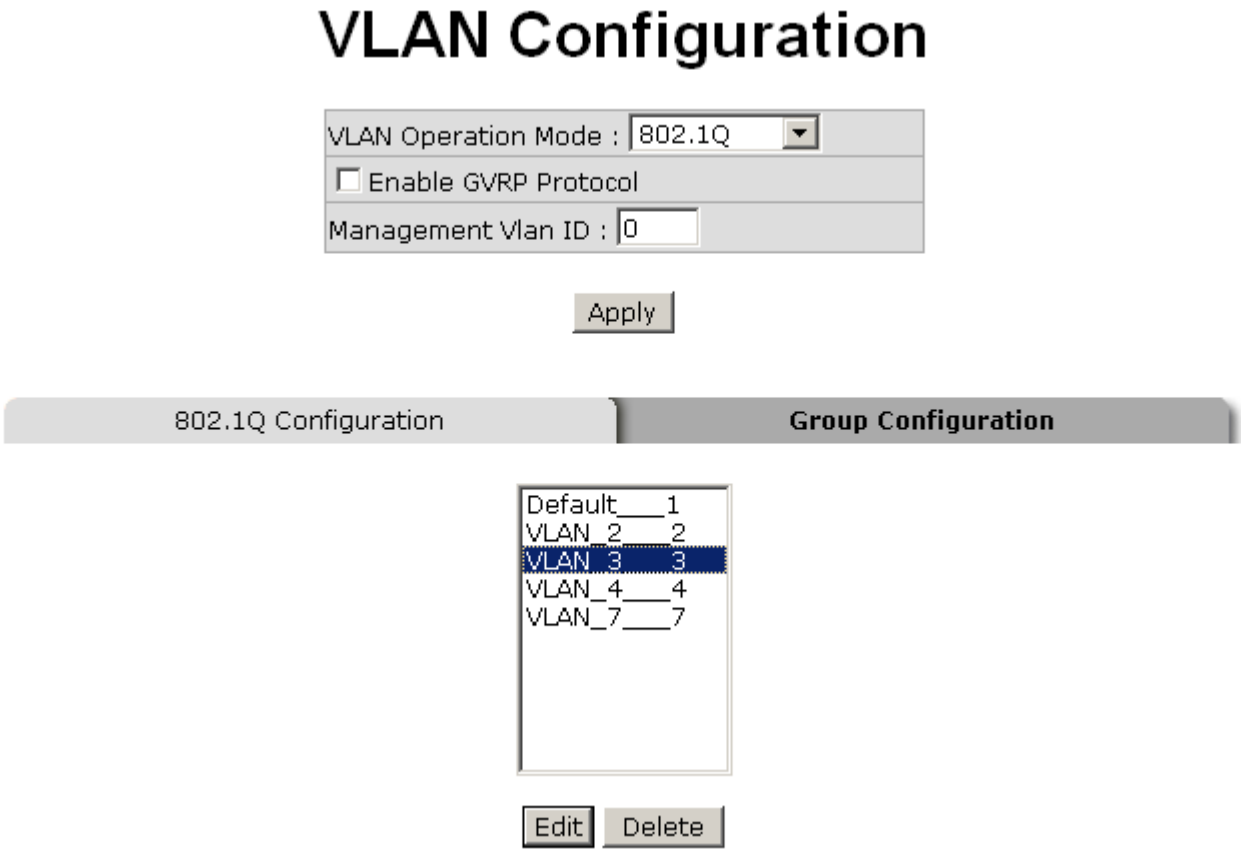


802.1Q VLAN interface

Group Configuration

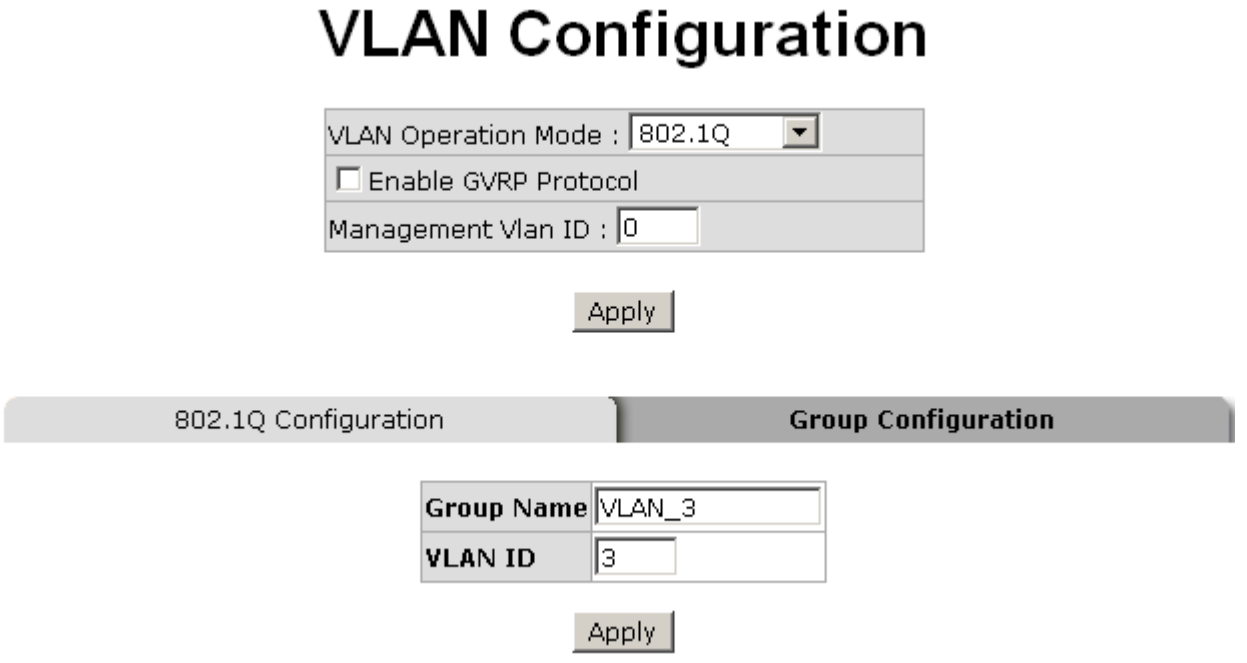
Edit the existing VLAN Group.

- Select the VLAN group in the table list.
- Click Edit.



Group Configuration interface

- You can modify the VLAN group name and VLAN ID.



Group Configuration interface

- Click Apply.

6.21 Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto-detect the connected device that is running STP or RSTP protocol.

6.21.1. System Configuration

- The user can view spanning tree information of Root Bridge.
- The user can modify RSTP state. After modification, click Apply.
  - **RSTP mode:** The user must enable the RSTP function first before configuring the related parameters.
  - **Priority (0-61440):** The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
  - **Max Age (6-40):** The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
  - **Hello Time (1-10):** The time that controls the switch to send out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
  - **Forward Delay Time (4-30):** The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

[NOTE]	Follow the rule as below to configure the MAX Age, Hello Time, and Forward Delay Time. **2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)**

RSTP - System Configuration

System Configuration | Port Configuration

RSTP Mode	Enable
Priority (0-61440)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096
2*(Forward Delay Time-1) should be greater than or equal to the Max Age.
The Max Age should be greater than or equal to 2*(Hello Time + 1).

Apply Help

Root Bridge Information

Bridge ID	0080001F3820820E
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

RSTP System Configuration interface

6.21.2. Port Configuration

This web page provides the port configuration interface for RSTP. You can assign higher or lower priority to each port. Rapid spanning tree will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

- Select the port in the port column field.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
- **Priority:** Decide which port should be blocked by setting its priority as the lowest. Enter a number between 0 and 240. The value of priority must be the multiple of 16.
- **Admin P2P:** The rapid state transitions possible within RSTP are dependent upon whether the port concerned can only be connected to exactly another bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means the port is regarded as a point-to-point link. False means the port is regarded as a shared link. Auto means the link type is determined by the auto-negotiation between the two peers.
- **Admin Edge:** The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
- **Admin Non Stp:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
- Click

.

RSTP - Port Configuration

System Configuration | **Port Configuration**

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	20000(	128	Auto	true	false

priority must be a multiple of 16

Apply Help

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	200000	128	True	True	False	Disabled	Disabled
Port.08	200000	128	True	True	False	Disabled	Disabled
Port.09	200000	128	True	True	False	Disabled	Disabled
Port.10	200000	128	True	True	False	Disabled	Disabled
Port.11	200000	128	True	True	False	Disabled	Disabled
Port.12	200000	128	True	True	False	Disabled	Disabled
Port.13	200000	128	True	True	False	Forwarding	Designated
Port.14	200000	128	True	True	False	Disabled	Disabled
Port.15	200000	128	True	True	False	Disabled	Disabled
Port.16	200000	128	True	True	False	Disabled	Disabled
Port.17	200000	128	True	True	False	Disabled	Disabled
Port.18	200000	128	True	True	False	Disabled	Disabled
Port.19	200000	128	True	True	False	Disabled	Disabled
Port.20	200000	128	True	True	False	Disabled	Disabled
Port.21	200000	128	True	True	False	Disabled	Disabled
Port.22	200000	128	True	True	False	Disabled	Disabled

RSTP Port Configuration interface

6.22 SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

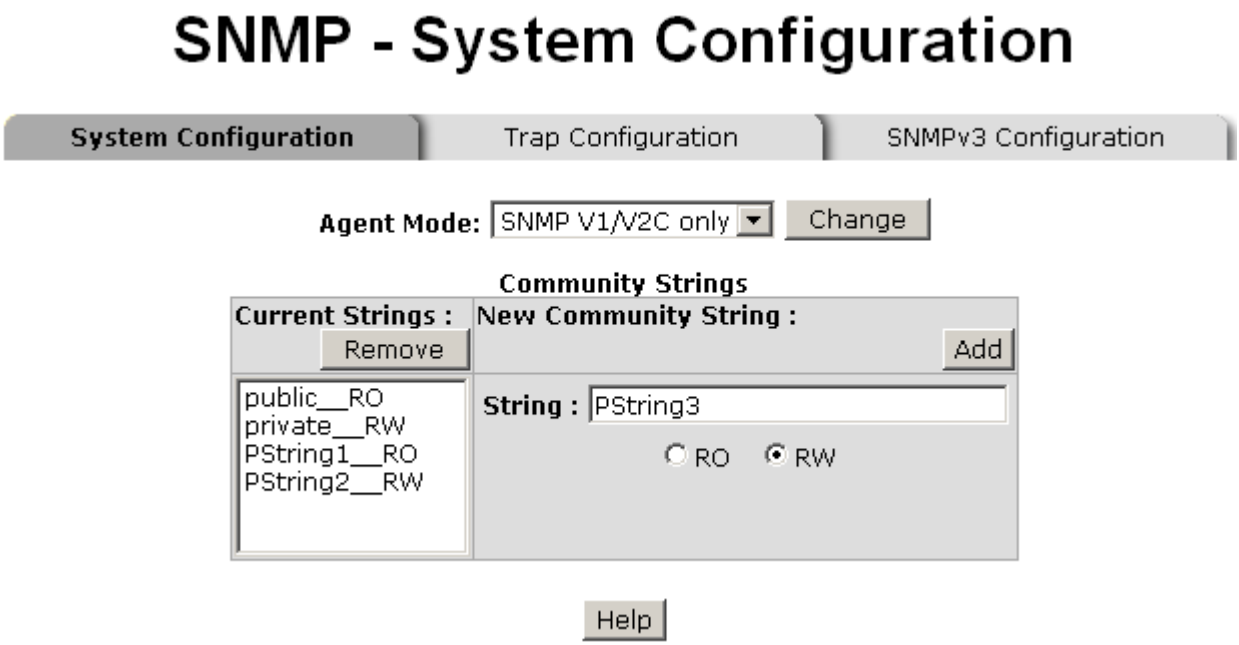
6.22.1. System Configuration

- **Agent Mode:** Select the SNMP version that you want to use and then click Change to have the selected SNMP version mode take effect. The default value is '**SNMP v1/v2c only**'.

- **Community Strings**

Here you can define the new community string set and remove the unwanted community string.

- **String:** Fill the name string.
- **RO:** Read only. Enables requests accompanied by this community string to display MIB-object information.
- **RW:** Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
- Click Add.
- To remove the community string, select the community string that you defined before and click Remove. The strings of Public_RO and Private_RW are default strings. You can remove them but after resetting the switch to default, the two strings show up again.

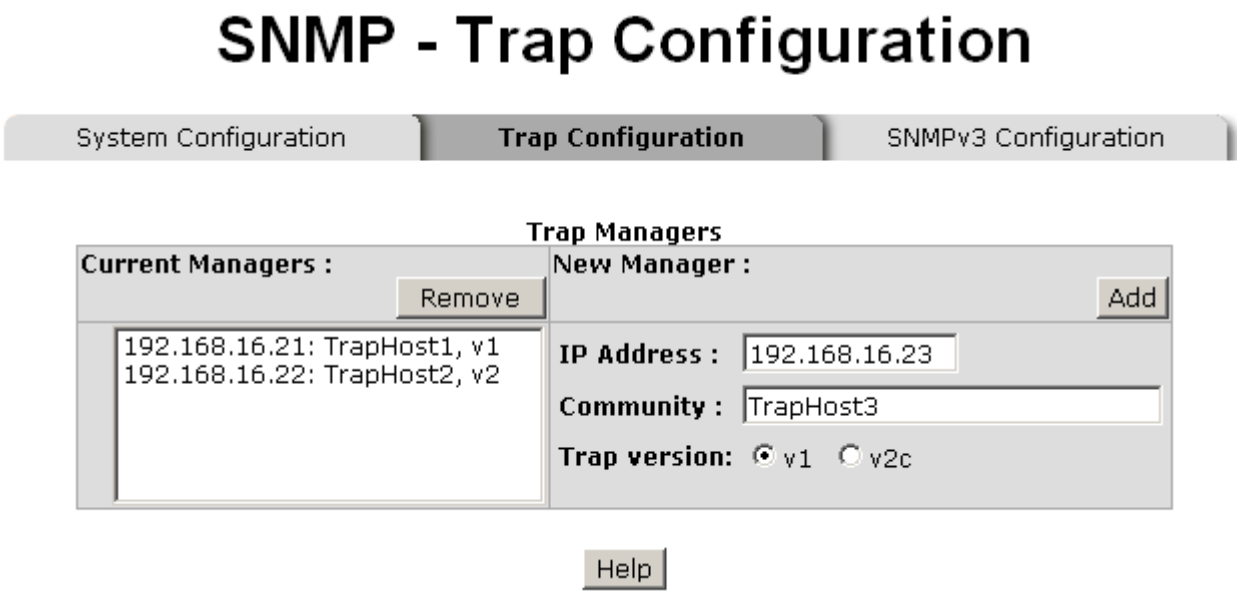


SNMP System Configuration interface

6.22.2. Trap Configuration

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

- **IP Address:** Enter the IP address of the trap manager.
- **Community:** Enter the community string for the trap station.
- **Trap Version:** Select the SNMP trap version type—v1 or v2c.
- Click Add.
- To remove the community string, select the community string listed in the current managers field and click Remove.



Trap Managers interface

6.22.3. SNMPV3 Configuration

Configure the SNMP V3 function.

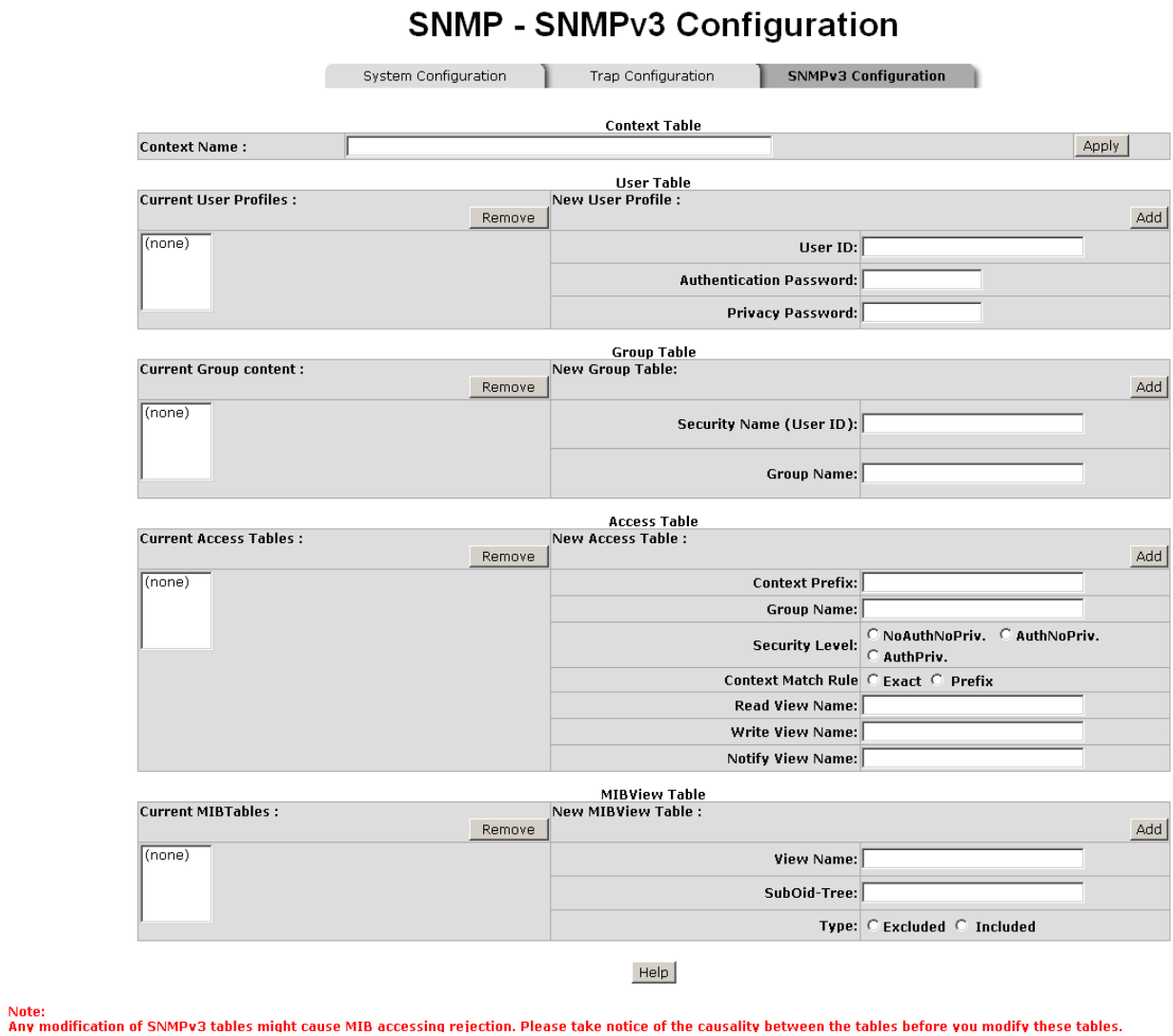
Context Table

Configure SNMP v3 context table. Assign the context name of context table. Click Add to add context name. Click Remove to remove the unwanted context name.

User Table

Configure SNMP v3 user table..

- **User ID:** Set up the user name.
- **Authentication Password:** Set up the authentication password.
- **Privacy Password:** Set up the private password.
- Click Add to add the context name.
- Click Remove to remove the unwanted context name.



SNMP V3 configuration interface

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in user table.
- **Group Name:** Set up the group name.
- Click Add to add the context name.
- Click Remove to remove the unwanted context name.

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Set up the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Click Add to add the context name.
- Click Remove to remove the unwanted context name.

MIBview Table

Configure MIB view table.

- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type—excluded or included.
- Click Add to add the context name.
- Click Remove to remove the unwanted context name.

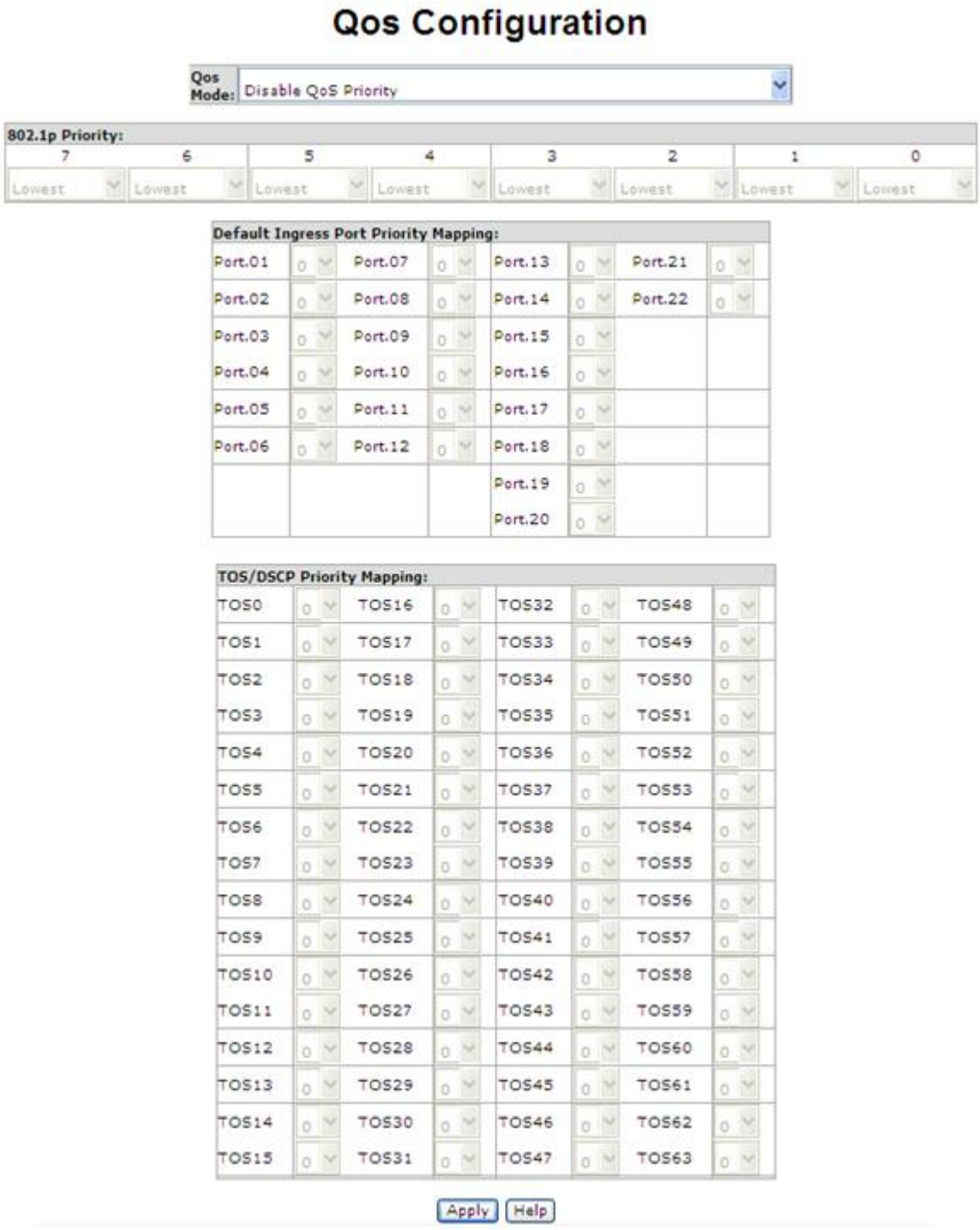
6.23 QoS Configuration

Quality of Service (QoS) is the ability to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP or Video Teleconferencing, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required.

- **QoS Mode:** Select the QoS policy rule.
  - **Disable Qos Priority:** The default status of QoS Priority is disabled.
  - **High Empty Then Low:** When all the high priority packets are empty in queue, low priority packets will be processed then.
  - **Highest:SecHigh:SecLow:Lowest=8:4:2:1:** The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example, while the system processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - **Highest:SecHigh:SecLow:Lowest=15:7:3:1:** Having set this QoS mode, the process order is in compliance with the transfer rate of 15:7:3:1.
  - **Highest:SecHigh:SecLow:Lowest=15:10:5:1:** Having set this QoS mode, the process order is in compliance with the transfer rate of 15:10:5:1.
  - Click Apply to have the configuration take effect.

- **802.1p priority [7-0]:** Configure per priority level. Priority 0 ~ 7: each priority has four priority levels—Highest, SecHigh, SecLow, and Lowest.
- **Default Ingress Port Priority Mapping:** Configure the priority level for each port. The port ingress level is between 0 and 7.
- **TOS/DSCP Priority Mapping:** The system provides 0 ~ 63 TOS priority level. Each level has 8 priorities—0 ~ 7. The default priority for each port is 0. When the IP packet is received, the system will check the TOS level value in the IP packet. For example,

TOS level 25 is set as 0 and each port only follows the TOS priority policy. When the packet received through all the ports on the switch, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25 (priority = 0), the packet priority has the highest priority.



QoS Configuration interface

6.24 IGMP Configuration

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch. IGMP have three fundamental types of message shown as follows:

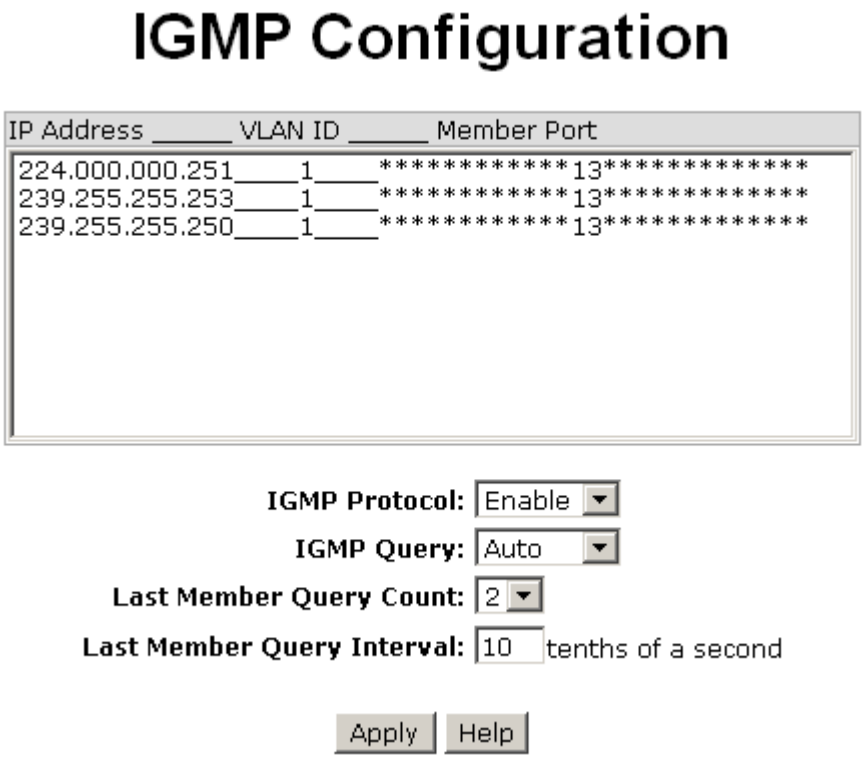
Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The switch supports IP multicast. You can enable IGMP protocol via setting the IGMP Configuration page to see the IGMP snooping information. IP multicast addresses are in the range of 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast networks.
- **Last Member Query Count:** This item allows the user to specify the query counts—1 or 2. If query count is set as 1, the switch will query whether any member is still in the IGMP group for sending one query after the query interval. With query count being set as 2, the switch will send two queries after the query interval.
- **Last Member Query Interval:** Fill in the number in seconds as the query interval

time.

- Click Apply.



IGMP Configuration interface

6.25 X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the X-Ring topology, every switch should be enabled with X-Ring function and two ports should be assigned as the member ports in the ring. Only one switch in the X-Ring group would be set as the master switch that one of its two member ports would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port of the master switch (Ring Master) will automatically become a working port to recover from the failure.

The switch supports the function and interface for setting the switch as the ring master or not. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, the software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode can be enabled by setting the X-Ring configuration interface. Also, the user can identify whether the switch is the ring master by checking the R.M. LED indicator on the panel of the switch.

The system also supports the **Couple Ring** that can connect 2 or more X-Ring group for the redundant backup function; **Dual Homing** function that can prevent connection lose between X-Ring group and upper level/core switch.

- **Enable Ring:** To enable the X-Ring function, tick the checkbox beside the Enable Ring string label. If this checkbox is not ticked, all the ring functions are unavailable.
  - **Enable Ring Master:** Tick the checkbox to enable this switch to be the ring master.
  - **1st & 2nd Ring Ports:** Pull down the selection menu to assign the ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically upgrade

the **2nd Ring Port** to be the working port.

- **Enable Couple Ring:** To enable the coupe ring function, tick the checkbox beside the Enable Couple Ring string label.
  - **Couple Port:** Assign the member port which is connected to the other ring group.
  - **Control Port:** When the **Enable Couple Ring** checkbox is ticked, you have to assign the control port to form a couple-ring group between the two X-rings.
- **Enable Dual Homing:** Set up one of the ports on the switch to be the Dual Homing port. For a switch, there is only one Dual Homing port. Dual Homing function only works when the X-Ring function enabled.
- And then, click Apply to have the configuration take effect.

X-ring Interface

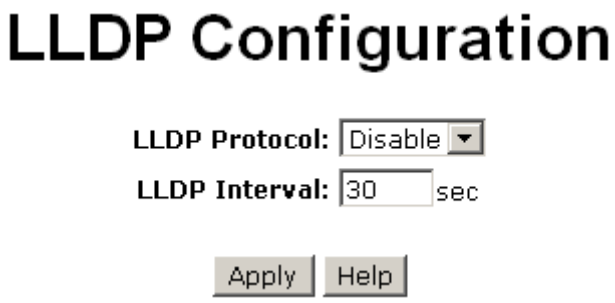
[NOTE]

1. When the X-Ring function enabled, the user must disable the RSTP. The X-Ring function and RSTP function cannot exist on a switch at the same time.
2. Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when switch powers off.

6.26 LLDP Configuration

Link Layer Discovery Protocol (LLDP) is defined in the IEEE 802.1AB, it is an emerging standard which provides a solution for the configuration issues caused by expanding LANs. LLDP specifically defines a standard method for Ethernet network devices such as switches, routers and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

- **LLDP Protocol**: Pull down the selection menu to disable or enable LLDP function.
- **LLDP Interval**: Set the interval of advertising the switch's information to other nodes.
- Click Apply.



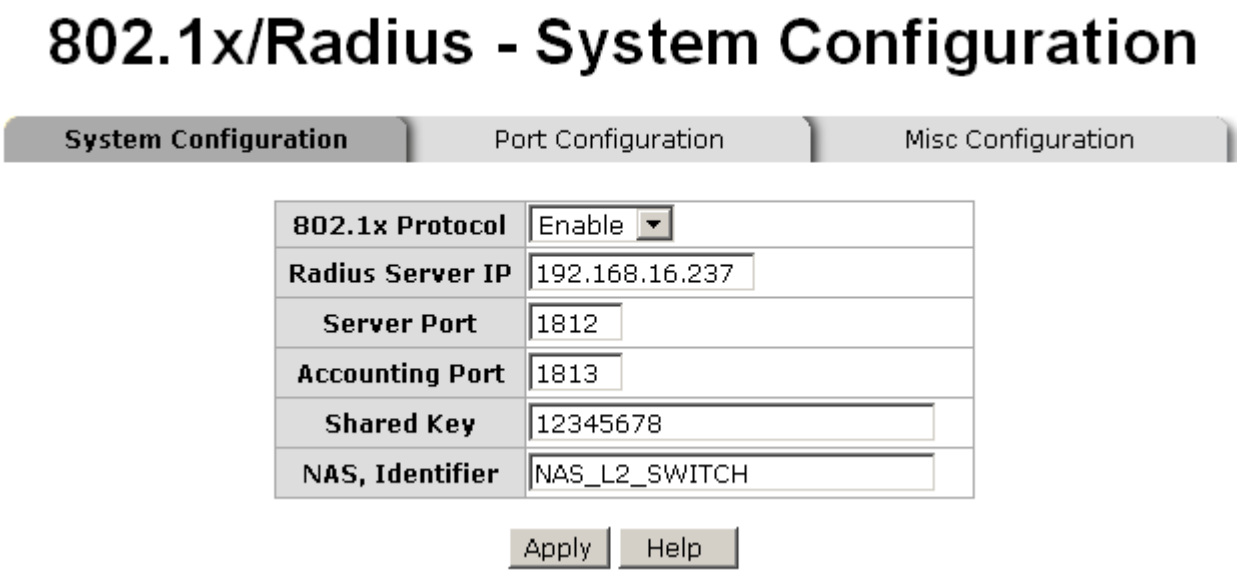
LLDP Interface

6.27 Security—802.1X/Radius Configuration

802.1x is an IEEE authentication specification which prevents the client from accessing a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

6.27.1. System Configuration

- **IEEE 802.1x Protocol:** Enable or disable 802.1x protocol.
- **Radius Server IP:** Assign the RADIUS Server IP address.
- **Server Port:** Set the UDP destination port for authentication requests to the specified RADIUS Server.
- **Accounting Port:** Set the UDP destination port for accounting requests to the specified RADIUS Server.
- **Shared Key:** Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
- **NAS, Identifier:** Set the identifier for the RADIUS client.
- Click Apply.

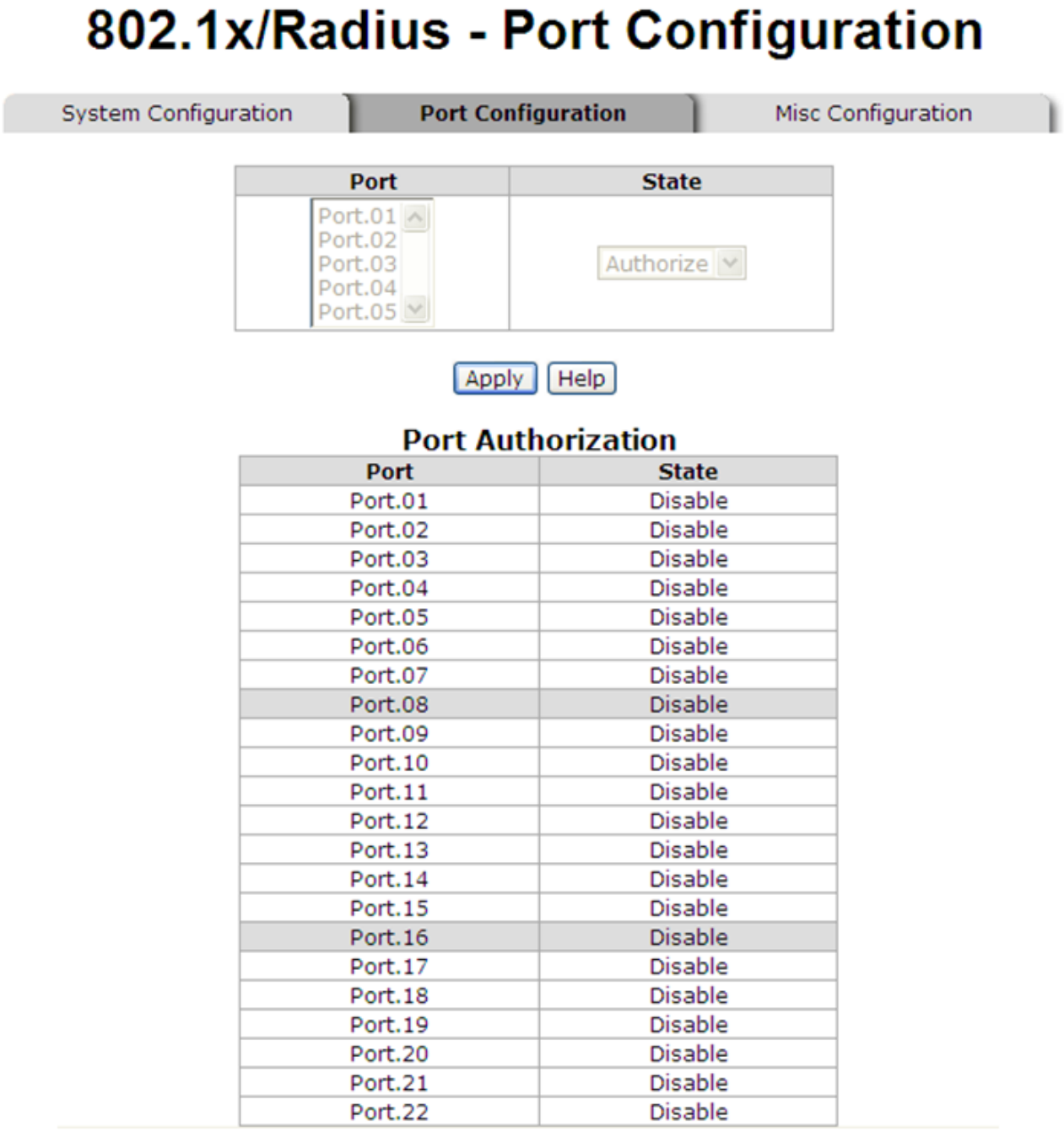


802.1x System Configuration interface

6.27.2. Port Configuration

You can configure the 802.1x authentication state for each port. The state provides Disable, Accept, Reject, and Authorize.

- **Reject:** The specified port is required to be held in the unauthorized state.
- **Accept:** The specified port is required to be held in the authorized state.
- **Authorize:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** When disabled, the specified port works without complying with 802.1x protocol.
- Click Apply.



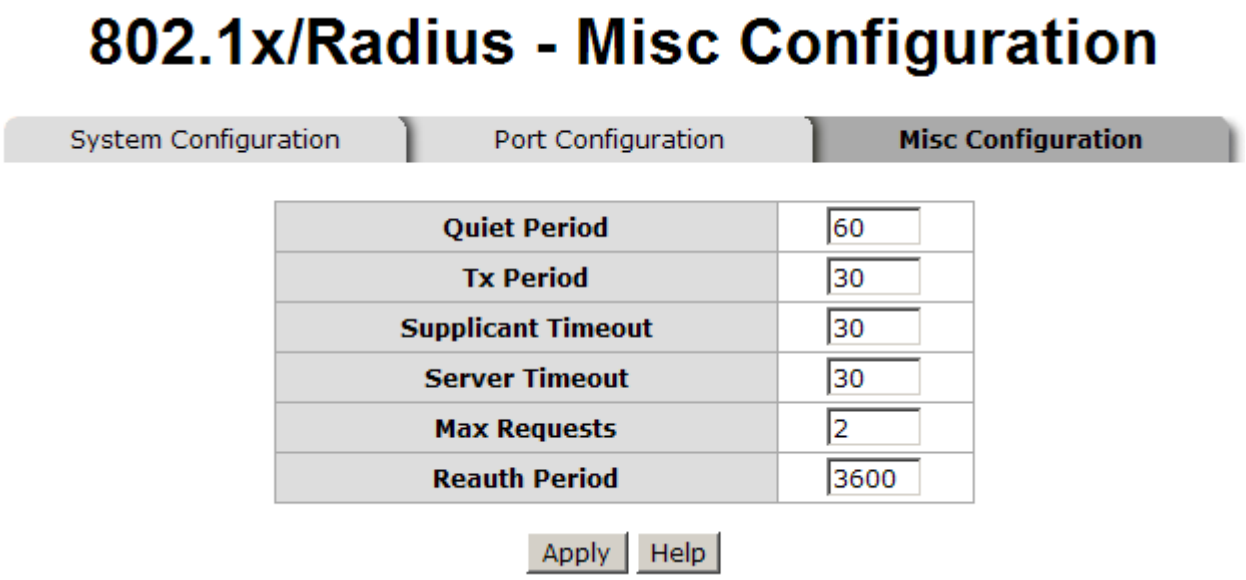
802.1x Per Port Setting interface

6.27.3. Misc Configuration

- **Quiet Period:** Set the period which the port doesn't try to acquire a supplicant.
- **TX Period:** Set the period the port waits for retransmit next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** Set the period of time the switch waits for a server response to

an authentication request.

- **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth period:** Set the period of time which clients connected must be re-authenticated.
- Click Apply.



802.1x Misc Configuration interface

6.28 MAC Address Table

Use the MAC address table to ensure the port security.

6.28.1. Static MAC Address

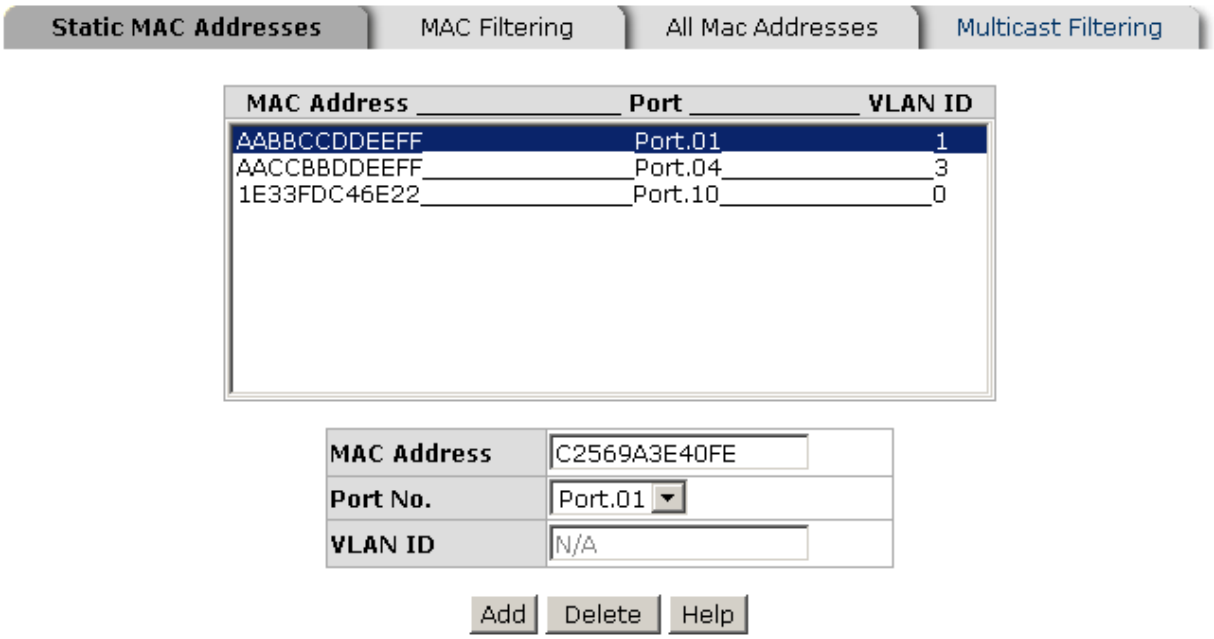
You can add a static MAC address that remains in the switch's address table regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. Via this interface, you can add / modify / delete a static MAC address.

Add the Static MAC Address

You can add static MAC address in the switch’s MAC table here. If the destination address and the VLAN ID of the packet meet the conditions set in the **Static MAC Addresses** table, the packet will be forwarded to the port only.

- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
- **Port No.:** Pull down the selection menu to select the port number to which the traffic will be forwarded.
- **VLAN ID:** Key in the VLAN ID to be the forwarding condition.
- Click Add.
- If you want to delete the MAC address from filtering table, select the MAC address and click Delete.

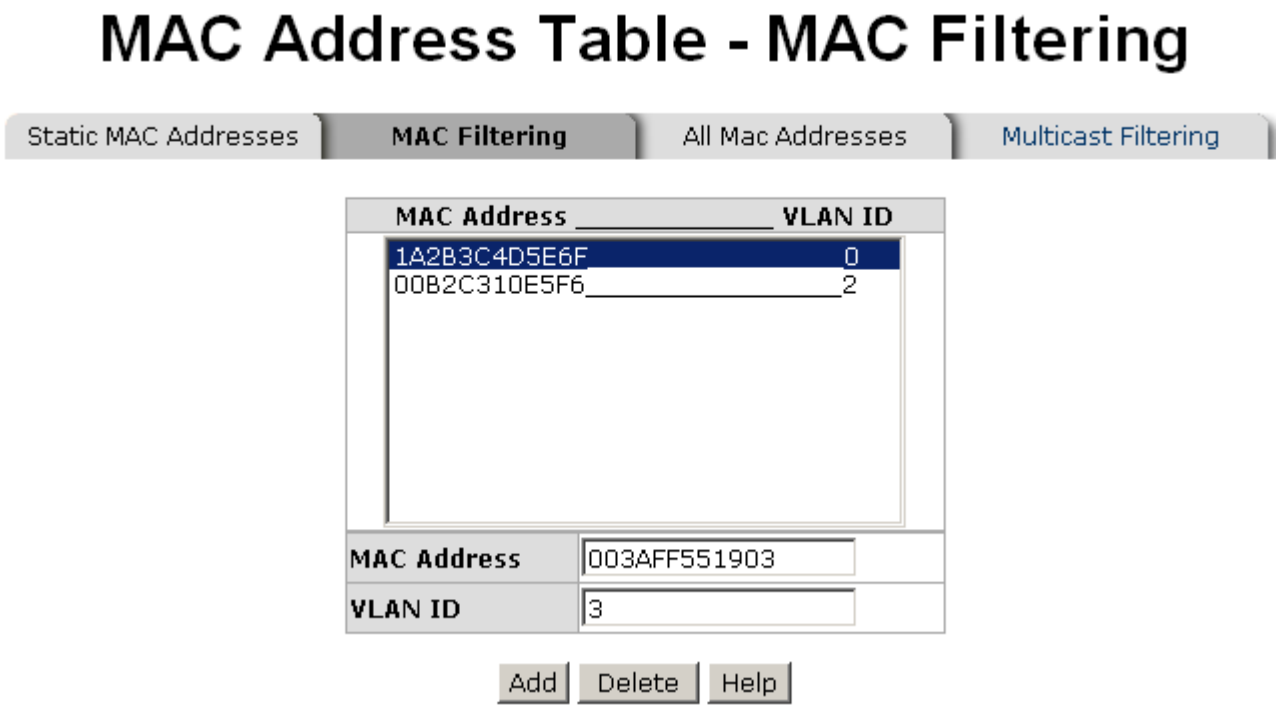
MAC Address Table - Static MAC Addresses



Static MAC Addresses interface

6.28.2. MAC Filtering

By filtering MAC address with VLAN ID, the switch will drop the packet when both its destination MAC address and VLAN ID meet the condition configured in the **MAC Filtering** table. You can add and delete the MAC filters.



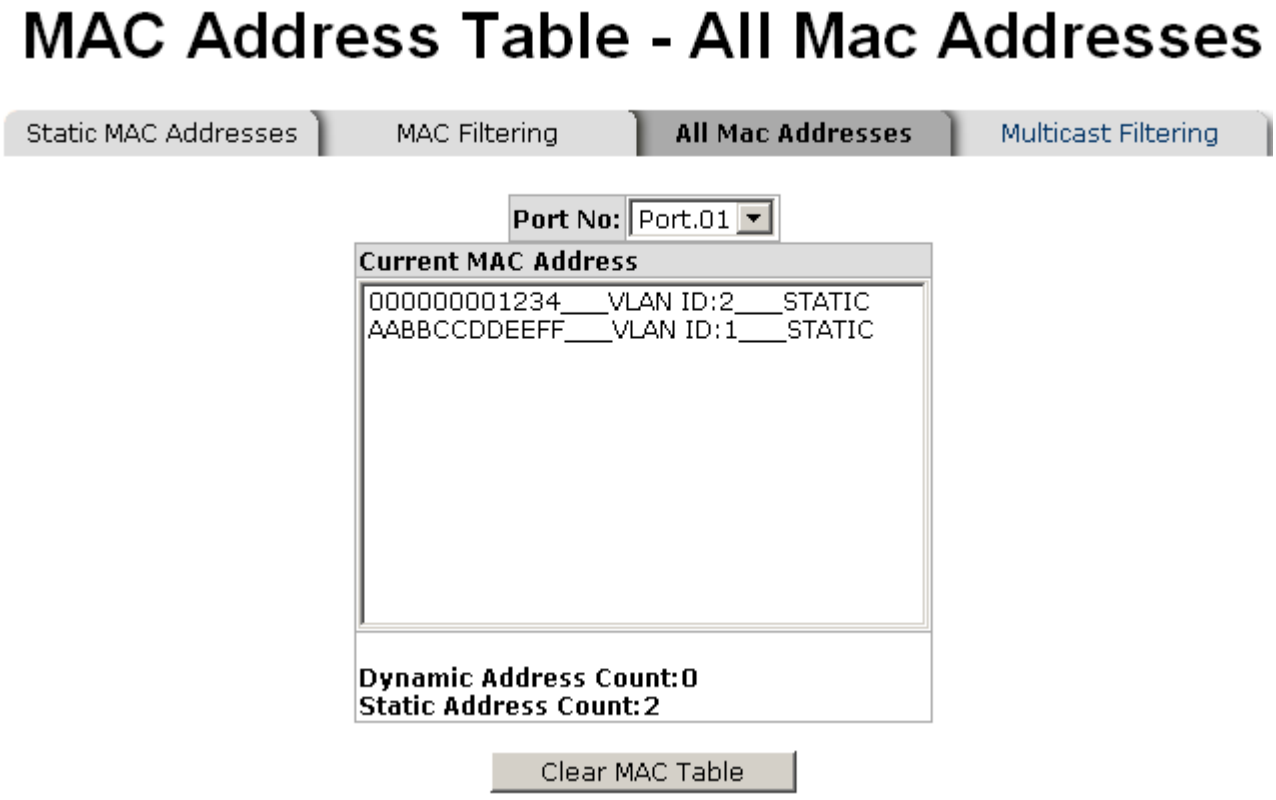
MAC Filtering interface

- **MAC Address:** Enter the MAC address that you want to filter.
- **VLAN ID:** Enter the VLAN ID that you want to filter.
- Click Add.
- If you want to delete the MAC address from the filtering table, select the MAC address and click Delete.

6.28.3. All MAC Addresses

You can view all of the MAC addresses learned by the selected port. This interface shows the MAC addresses information group by port.

- **Port No.:** Select the port number to view its MAC address.
- **Current MAC Address:** The static & dynamic MAC address information of the selected port will be displayed in here.
- Click Clear MAC Table to clear the dynamic MAC addresses information of the current port.



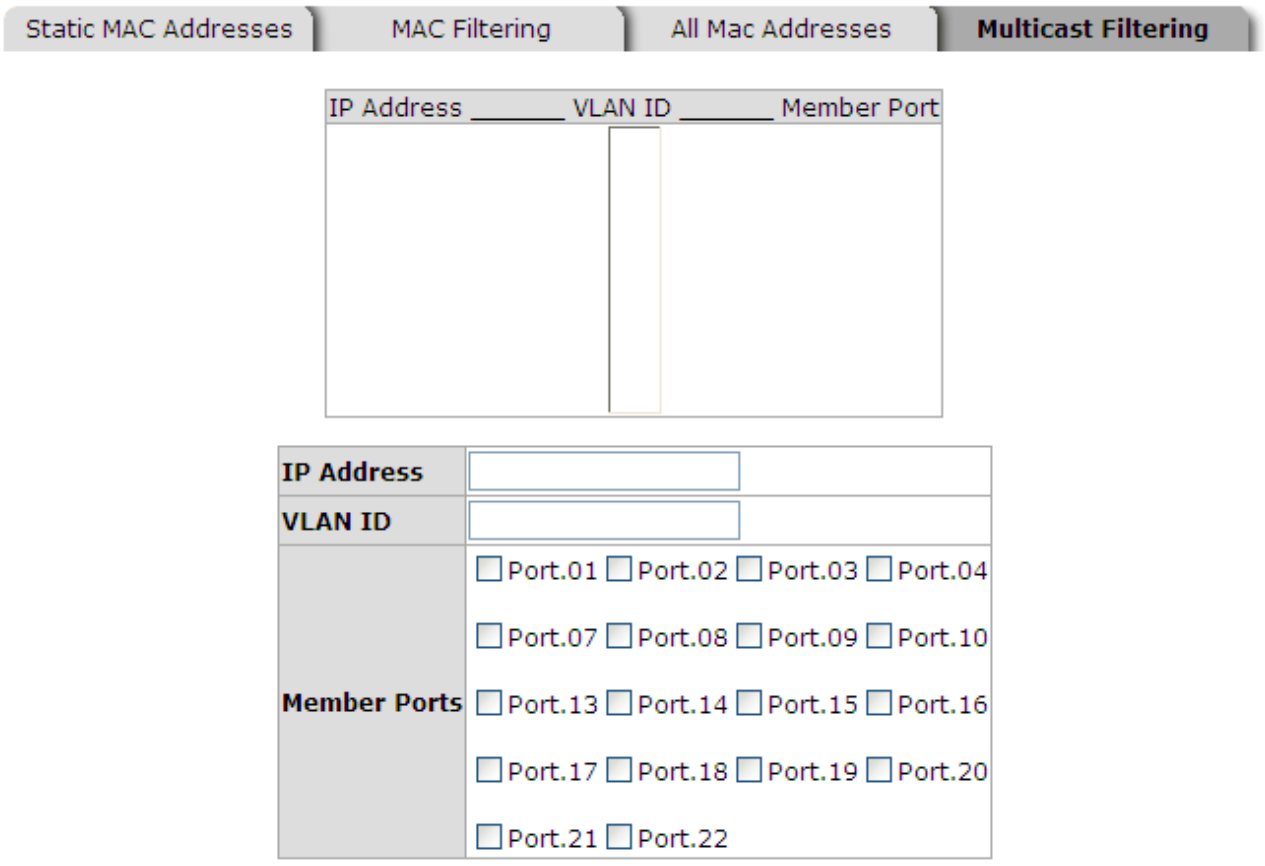
All MAC Address interface

6.28.4. MAC Address Table—Multicast Filtering

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

- **IP Address**: Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
- **VLAN ID**: Assign a VLAN ID that limit the source and destination ports must belong to the same VLAN. Therefore, the packet meets the conditions will then be forwarded to the destination port.
- **Member Ports**: Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
- Click Add to append a new filter of multicast to the field, or select the filter in the field and click Delete to remove it.

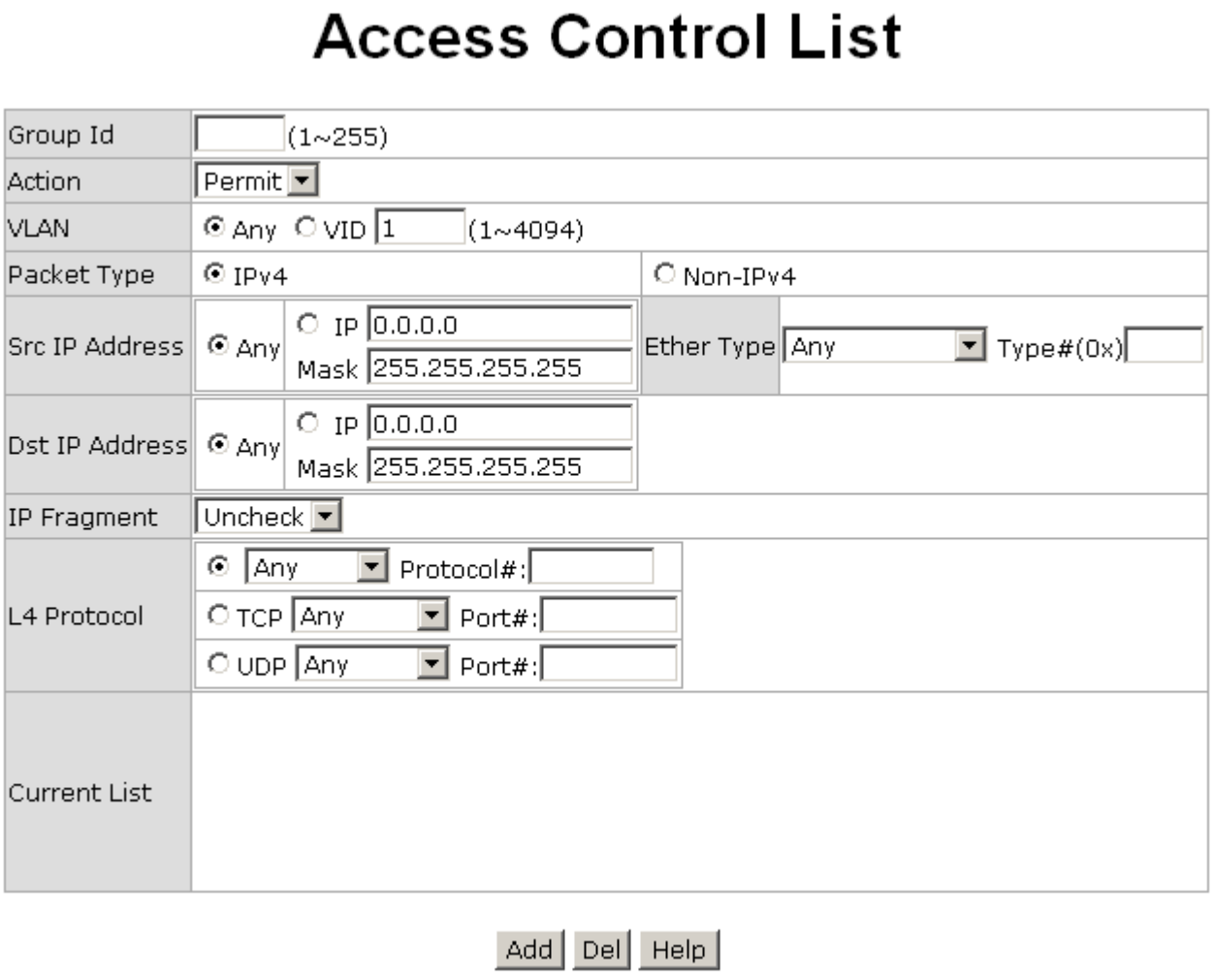
MAC Address Table - Multicast Filtering



Multicast Filtering interface

6.29 Access Control List

- **Group Id:** Type in the Group ID from 1 to 255.
- **Action:** Permit and Deny.
- **VLAN:** Select any or a particular VID.
- **Packet type:** Select packet type—IPv4 or Non-IPv4
- **Src IP Address:** Select any or assign an IP address with Subnet Mask for source IP address.
- **Dst IP Address:** Select any or assign an IP address with Subnet Mask for destination IP address.
- **Ether Type:** Pull down the select menu for Any, ARP or IPX.
- **IP Fragment:** Set this item as to whether the fragment is checked or not.
- **L4 Protocol:** Assign the L4 protocol from among ICMP(1), IGMP(2), TCP or UDP.
- **Current List:** Displays the current list information.



Access Control List interface

6.30 Factory Default

Reset switch to default configuration. Click Reset to reset all configurations to the default value.

Factory Default interface

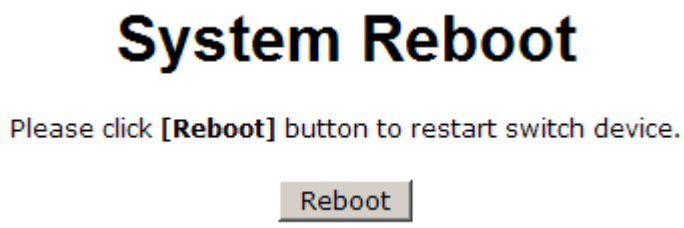
6.31 Save Configuration

Save all configurations that you have made in the system. To ensure the all configuration will be saved. Click Save to save the all configuration to the flash memory.

Save Configuration interface

6.32 System Reboot

Reboot the switch in software reset. Click Reboot to reboot the system.



System Reboot interface

Troubleshooting

- Verify that you are using the right power cord/adapter. The power output of the adapter can't be higher than the power rating of the equipment. Otherwise, the equipment will burn down.
- Select the proper UTP/STP cable to construct the user network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections that depend on the connector type the switch equipped: 100Ω Category 3, 4 or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps connections, or 100Ω Category 5e/above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- **Diagnosing LED Indicators:** To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.
- If the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact the local dealer for assistance.
- If the LED indicators are normal and the connected cables are correct but the packets still cannot be transmitted. Please check the user system's Ethernet devices' configuration or status.

Appendix A — RJ-45 Pin Assignment

- **RJ-45 ports**

The UTP/STP ports will automatically sense for Fast Ethernet (10Base-T/100Base-TX connections), or Gigabit Ethernet (10Base-T/100Base-TX/1000Base-T connections). Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling. See the figures below for straight through and crossover cable schematic.

- **10 /100BASE-TX Pin outs**

With10/100BASE-TX cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

- **RJ-45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

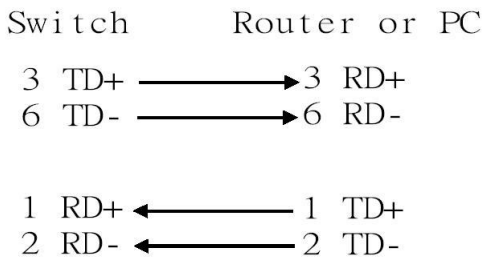
[NOTE] "+" and "-" signs represent the polarity of the wires that make up each wire pair.

The table below shows the 10/100BASE-TX MDI and MDI-X port pin outs.

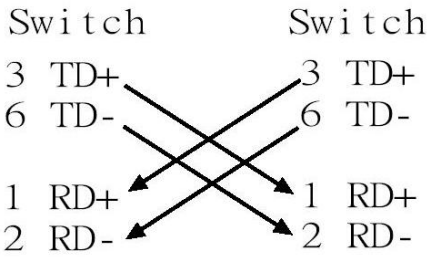
Pin Number	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)

■ 10/100Base-TX Cable Schematic

The following two figures show the 10/100Base-TX cable schematic.



Straight-through cable schematic

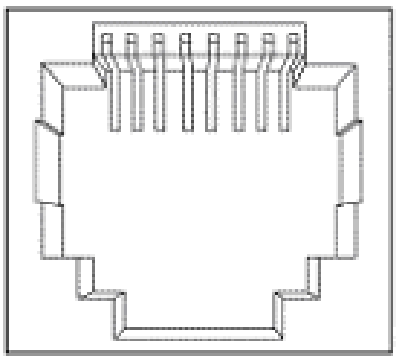


Cross over cable schematic

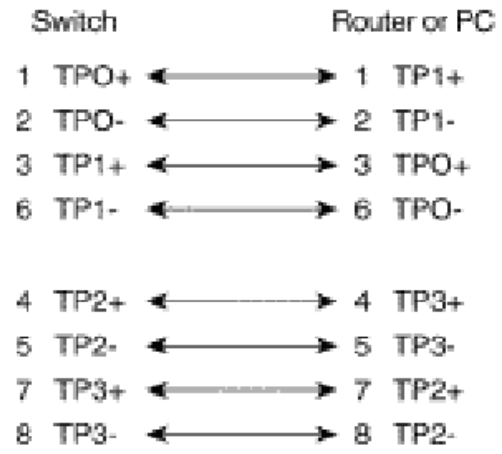
■ 10/100/1000Base-TX Pin outs

The following figure shows the 10/100/1000 Ethernet RJ-45 pin outs.

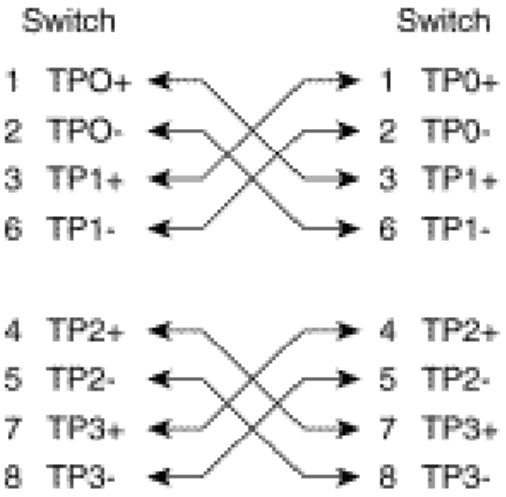
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



■ 10/100/1000Base-TX Cable Schematic



Straight through cables schematic



Cross over cables schematic

Appendix B — Command Sets

Commands Set List

User EXEC	**E**
Privileged EXEC	**P**
Global configuration	**G**
VLAN database	**V**
Interface configuration	**I**

System Commands Set

Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>**show config**
show terminal	**P**	Show console information	switch#**show terminal**
write memory	**G**	Save user configuration into permanent memory (flash rom)	switch#**write memory**
system name **[System Name]**	**G**	Configure system name	switch(config)#**system name xxx**
system location **[System Location]**	**G**	Set switch system location string	switch(config)#**system location xxx**
system description **[System Description]**	**G**	Set switch system description string	switch(config)#**system description xxx**
system contact **[System Contact]**	**G**	Set switch system contact window string	switch(config)#**system contact xxx**
show system-info	**E**	Show system information	switch>**show system-info**
ip address	**G**	Configure the IP	switch(config)#**ip address**

[Ip-address] [Subnet-mask] [Gateway]		address of switch	**192.168.1.1 255.255.255.0 192.168.1.254**
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#**ip dhcp**
show ip	**P**	Show IP information of switch	switch#**show ip**
no ip dhcp	**G**	Disable DHCP client function of switch	switch(config)#**no ip dhcp**
reload	**G**	Halt and perform a cold restart	switch(config)#**reload**
default	**G**	Restore to default	Switch(config)#**default**
admin username [Username]	**G**	Changes a login username. (maximum 10 words)	switch(config)#**admin username xxxxxx**
admin password [Password]	**G**	Specifies a password (maximum 10 words)	switch(config)#**admin password xxxxxx**
show admin	**P**	Show administrator information	switch#**show admin**
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#**dhcpserver enable**
dhcpserver lowip [Low IP]	**G**	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.1**
dhcpserver highip [High IP]	**G**	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.1.50**
dhcpserver subnetmask [Subnet mask]	**G**	Configure subnet mask for DHCP clients	switch(config)#**dhcpserver subnetmask 255.255.255.0**
dhcpserver gateway [Gateway]	**G**	Configure gateway for DHCP clients	switch(config)#**dhcpserver gateway 192.168.1.254**
dhcpserver dnsip [DNS IP]	**G**	Configure DNS IP for DHCP clients	switch(config)#**dhcpserver dnsip 192.168.1.1**
dhcpserver leasetime [Sec.]	**G**	Configure lease time (in sec.)	switch(config)#**dhcpserver leasetime 1**

dhcpserver ipbinding [IP address]	**I**	Set static IP for DHCP clients by port	switch(config)#**interface fastEthernet 2** switch(config-if)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#**show dhcpserver configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#**show dhcpserver clinets**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	**G**	Enable IP security function	switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch(config)#**security telnet**
security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch(config)#**security ip 1 192.168.1.55**
show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**
no security http	**G**	Disable IP security of HTTP server	switch(config)#**no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)#**no security telnet**
bsf rate	**G**	Configure Broadcast Storm Filter selection	switch(config)#**bsf rate 1/2**
bsf flooded-unicast-	**G**	Enable Flooded	switch(config)#**bsf flooded-**

multicast		Unicast/Multicast Packets BSF	**unicast-multicast**
bsf control	**G**	Enable Control Packets BSF	switch(config)#**bsf control**
bsf ip-multicast	**G**	Enable IP Multicast Packets BSF	switch(config)#**bsf ip-multicast**
bsf broadcast	**G**	Packets BSF	switch(config)#**bsf broadcast**
no bsf flooded-unicast-multicast	**G**	Disable Flooded Unicast/Multicast Packets BSF	switch(config)#**no bsf flooded-unicast-multicast**
no bsf control	**G**	Disable Control Packets BSF	switch(config)#**no bsf control**
no bsf ip-multicast	**G**	Disable IP Multicast Packets BSF	switch(config)#**no bsf ip-multicast**
no bsf broadcast	**G**	Disable Broadcast Packets BSF	switch(config)#**no bsf broadcast**
jumbo-frame	**G**	Enable jumbo frame	switch(config)#**jumbo-frame**
no jumbo-frame	**G**	Disable jumbo frame	switch(config)#**no jumbo-frame**
show jumbo-frame	**G**	Show jumbo frame enable/disable	switch#**show jumbo-frame**

Port Commands Set

Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#**interface fastEthernet 2**
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet, the speed can't be set to 1000 if the port isn't a giga port.	switch(config)#**interface fastEthernet 2** switch(config-if)#**speed 100**
flowcontrol [Enable|Disable]	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#**interface fastEthernet 2** switch(config-if)#**flowcontrol enable**
no flowcontrol	I	Disable flow control of interface	switch(config-if)#**no flowcontrol**
security enable	I	Enable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**security enable**
no security	I	Disable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**no security**
ratelimit in [Value]	I	Set interface input rate limiting	switch(config)#**interface fastEthernet 2** switch(config-if)#**ratelimit in 100**

ratelimit out [Value]		Set interface output rate limiting	switch(config)#**interface fastEthernet 2** switch(config-if)#**ratelimit out 100**
show ratelimit	**I**	Show interfaces rate limiting	switch(config)#**interface fastEthernet 2** switch(config-if)#**show ratelimit**
state [Enable | Disable]	**I**	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#**interface fastEthernet 2** switch(config-if)#**state Disable**
show interface configuration	**I**	show interface configuration status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface configuration**
show interface status	**I**	show interface actual status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface status**
show interface accounting	**I**	show interface statistic counter1	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface accounting**
no accounting	**I**	Clear interface accounting information	switch(config)#**interface fastEthernet 2** switch(config-if)#**no accounting**
alias [name]	**I**	Configure alias name of port	switch(config)#**interface fastEthernet 2** switch(config-if)#**alias PORT002**

Trunk Commands Set

Commands	Level	Description	Example
aggregator priority [1~65535]	G	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator activityport [Group ID][Port Numbers]	G	Set activity port	switch(config)#**aggregator activityport 2 2**
aggregator group [GroupID] [Port-list] **lacp workp** [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**
aggregator group [GroupID] [Port-list] **nolacp**	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggreator group 1 3,1,2 nolacp**

show aggregator **[Group-number]**	**P**	Show the information of trunk group	switch#**show aggregator 1**
no aggregator lacp **[GroupID]**	**G**	Disable the LACP function of trunk group	switch(config)#**no aggreator lacp 1**
no aggregator group **[GroupID]**	**G**	Remove a trunk group	switch(config)#**no aggreator group 2**

VLAN Commands Set

Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#**vlan database**
vlanmode [portbase| 802.1q | gvrp]	**V**	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
no vlan	**V**	Disable VLAN	Switch(vlan)#**no vlan**
Ported based VLAN configuration			
vlan port-based grpname [Group Name] grpid [GroupID] port [PortNumbers]	**V**	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	**V**	Delete port base group ID	switch(vlan)#**no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] vid [VID]	**V**	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#**vlan 8021q name test vid 22**
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	**V**	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 access-link untag 33**

vlan 8021q port **[PortNumber]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by port. If the port belongs to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port **[PortNumber]** **hybrid-link untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk **[Trunk ID]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 access-link untag 33**
vlan 8021q trunk **[Trunk ID]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 3-20**
vlan 8021q trunk **[Trunk ID]** **hybrid-link untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group **[GroupID]**	**V**	Delete port base group ID	switch(vlan)#**no vlan group 2**

Spanning Tree Commands Set

Commands	Level	Description	Example
spanning-tree enable	**G**	Enable spanning tree	switch(config)#**spanning-tree enable**
spanning-tree priority [0~61440]	**G**	Configure spanning tree priority parameter	switch(config)#**spanning-tree priority 32768**
spanning-tree max-age [seconds]	**G**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)#**spanning-tree max-age 15**
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#**spanning-tree hello-time 3**
spanning-tree forward-time [seconds]	**G**	Use the spanning-tree forward-time global configuration command	switch(config)#**spanning-tree forward-time 20**

		to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	
stp-path-cost **[1~200000000]**	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**
stp-path-priority **[Port Priority]**	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-priority 127**
stp-admin-p2p	**I**	Admin P2P of STP	switch(config)#**interface**

[Auto|True|False]		priority on this interface.	**fastEthernet 2** switch(config-if)#**stp-admin-p2p Auto**
stp-admin-edge **[True|False]**	**I**	Admin Edge of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-edge True**
stp-admin-non-stp **[True|False]**	**I**	Admin NonSTP of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-non-stp False**
show spanning-tree	**E**	Display a summary of the spanning-tree states.	switch>**show spanning-tree**
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#**no spanning-tree**

QOS Commands Set

Commands	Level	Description	Example
qos priority-tos **[TosNum][Priority]**	**G**	Configure TOS Priority	switch(config)#**qos priority-tos 9 7**
qos mode **[SP|WRR|WRR1|WRR2]**	**G**	Configure QOS mode	switch(config)#**qos mode sp**
qos 8021p-priority **[Index][Lowest|SecLow |SecHigh|Highest]**	**G**	Configure 8021p Priority	switch(config)#**qos 8021p-Priority 1 lowest**
qos priority-portbased **[Priority]**	**I**	Configure COS Priority	switch(config)#**interface fastEthernet 2** switch(config-if)#**qos priority-portbased 1**

IGMP Commands Set

Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#**igmp enable**
Igmp-query auto	G	Set IGMP query to auto mode	switch(config)#**igmp-query auto**
Igmp-query force	G	Set IGMP query to force mode	switch(config)#**igmp-query**
igmp last-query-count [1~2]	G	Configure last member query count	switch(config)#**igmp last-query-count 1**
igmp last-query-interval [1~250 tenths of a sec.]	G	Configure last member query interval	switch(config)#**igmp last-query-interval 60**
show igmp configuration	P	Show IGMP configuration	switch#**show igmp configuration**
show igmp multi	P	Show IGMP multicast table	switch#**show igmp multi**
no igmp	G	Disable IGMP snooping function	switch(config)#**no igmp**
no igmp-query	G	Disable IGMP query	switch#**no igmp-query**

Mac / Filter Table Commands Set

Commands	Level	Description	Example
mac-address-table static hwaddr [HW-Addr][VID]	I	Configure MAC address table of interface (static).	switch(config)#**interface fastEthernet 2** switch(config-if)#**mac-address-table static hwaddr 000012345678 1**
mac-address-table filter hwaddr [HW-Addr][VID]	G	Configure MAC address table(filter)	switch(config)#**mac-address-table filter hwaddr 000012348678 1**
show mac-address-table	I	Show all MAC address table	switch(config)#**interface fastEthernet 2** switch(config-if)#**show mac-address-table**
show mac-address-table static	P	Show static MAC address table	switch#**show mac-address-table static**
show mac-address-table filter	P	Show filter MAC address table.	switch#**show mac-address-table filter**
no mac-address-table static hwaddr [HW-Addr][VID]	I	Remove an entry of MAC address table of interface (static)	switch(config)#**interface fastEthernet 2** switch(config-if)#**no mac-address-table static hwaddr 000012345678 1**
no mac-address-table filter hwaddr [HW-Addr][VID]	G	Remove an entry of MAC address table (filter)	switch(config)#**no mac-address-table filter hwaddr 000012348678 1**
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#**no mac-address-table**
auto-age [150|300|600]	G	Configure auto age time of MAC table	switch(config)#**auto-age 150**
no auto-age	G	Disable auto age time of MAC table	switch(config)#**no auto-age**
show auto-age	P	Display auto age time	switch#**show auto-age**

		of MAC table	
auto-flush	**G**	Enable auto flush MAC Table when link down	switch(config)#**auto-flush**
no auto-flush	**G**	Disable auto flush MAC Table when link down	switch(config)#**no auto-flush**
show auto-flush	**P**	Disable auto flush function of MAC table	switch#**show auto-flush**
multicast-filtering **[IP-Addr][VID]**	**I**	Configure multicast filtering entry of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**multicast-filtering 239.0.0.1 1**
no multicast-filtering **[IP-Addr][VID]**	**I**	Remove multicast filtering entry of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**no multicast-filtering 239.0.0.1 1**
no multicast-filtering **[IP-Addr][VID]**	**G**	Remove multicast filtering entry	switch(config)#**no multicast-filtering 239.0.0.1 1**
show multicast-filtering	**I**	Show multicast filtering table	switch#**show multicast-filtering**

SNMP Commands Set

Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#**snmp system-name l2switch**
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#**snmp system-location lab**
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#**snmp system-contact where**
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#**snmp agent-mode v1v2cv3**
snmp community-strings [Community] **right** [RO/RW]	G	Add SNMP community string.	switch(config)#**snmp community-strings public right rw**
snmp-server host [IP address] **community** [Community-string] **trap-version** [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#**snmp-server host 192.168.1.50 community public trap-version v1** (remove) Switch(config)#**no snmp-server host 192.168.1.50**
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#**snmpv3 context-name Test**
snmpv3 user [User Name] **group** [Group Name] **password** [Authentication Password] [Privacy Password]	G	Configure the user profile for SNMPV3 agent. Privacy password could be empty.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**
snmpv3 access context-name [Context Name]	G	Configure the access table of SNMPV3 agent	switch(config)#**snmpv3 access context-name Test group G1 security-level AuthPriv**

group [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]			**match-rule Exact views V1 V1 V1**
snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	**G**	Configure the mibview table of SNMPV3 agent	switch(config)#**snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**
show snmp	**P**	Show SNMP configuration	switch#**show snmp**
no snmp community-strings [Community]	**G**	Remove the specified community.	switch(config)#**no snmp community-strings public**
no snmp-server host [Host-address]	**G**	Remove the SNMP server host.	switch(config)#**no snmp-server host 192.168.1.50**
no snmpv3 user [User Name]	**G**	Remove specified user of SNMPv3 agent.	switch(config)#**no snmpv3 user Test**
no snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPr iv match-rule Exact views V1 V1 V1**

match-rule **[Exact|Prifix]** **views** **[Read View Name]** **[Write View Name]** **[Notify View Name]**			
no snmpv3 mibview view **[View Name]** **type** **[Excluded|Included]** **sub-oid** **[OID]**	**G**	Remove specified mibview table of SNMPV3 agent.	switch(config)#**no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

Port Mirroring Commands Set

Commands	Level	Description	Example
monitor destination **[Port ID]**	**G**	Set destination port	switch(config)#**monitor destination 1**
monitor source **[Port ID]**	**G**	Set source port	switch(config)#**monitor source 2**
monitor mode **[RX|TX|Both|Disabled]**	**G**	Configure mode of monitor function	switch(config)#**monitor mode rx**
show monitor	**P**	Show port monitor information	switch#**show monitor**

802.1x Commands Set

Commands	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)#**8021x enable**
8021x system radiousip [IP address]	**G**	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)#**8021x system radiousip 192.168.1.1**
8021x system serverport [Port Number]	**G**	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)#**8021x system serverport 1812**
8021x system accountport [Port Number]	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)#**8021x system accountport 1813**
8021x system sharedkey [SharedKey]	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)#**8021x system sharedkey 123456**
8021x system nasid [NAS ID]	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)#**8021x system nasid test1**

8021x misc quietperiod [sec.]	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)#**8021x misc quietperiod 10**
8021x misc txperiod [sec.]	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)#**8021x misc txperiod 5**
8021x misc supptimeout [sec.]	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)#**8021x misc supptimeout 20**
8021x misc servertimeout [sec.]	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#**8021x misc servertimeout 20**
8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)#**8021x misc maxrequest 3**
8021x misc reauthperiod [sec.]	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)#**8021x misc reauthperiod 3000**

8021x portstate [disable | reject | accept | authorize]	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#**interface fastethernet 2** switch(config-if)#**8021x portstate accept**
show 8021x	**E**	Display a summary of the 802.1x properties and also the port sates.	switch>**show 8021x**
no 8021x	**G**	Disable 802.1x function	switch(config)#**no 8021x**

TFTP Commands Set

Commands	Level	Description	Example
backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**backup flash:backup_cfg**
restore flash:restore_cfg	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#**restore flash:restore_cfg**
upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**upgrade flash:upgrade_fw**

SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
systemlog ip [IP address]	G	Set System log server IP address.	switch(config)#**systemlog ip 192.168.1.100**
systemlog mode [client|server|both]	G	Specified the log mode	switch(config)#**systemlog mode both**
show systemlog	E	Display system log.	Switch>**show systemlog**
show systemlog	P	Show system log client & server information	switch#**show systemlog**
no systemlog	G	Disable systemlog functon	switch(config)#**no systemlog**
smtp enable	G	Enable SMTP function	switch(config)#**smtp enable**
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#**smtp serverip 192.168.1.5**
smtp subject [subject]	G	Configure subject of mail	switch(config)#**smtp subject test**
smtp sender [sender]	G	Configure sender of mail	switch(config)#**smtp sender tester**
smtp authentication	G	Enable SMTP authentication	switch(config)#**smtp authentication**
smtp account [account]	G	Configure authentication account	switch(config)#**smtp account User**
smtp password [password]	G	Configure authentication password	switch(config)#**smtp password**
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#**smtp rcptemail 1 Alert@test.com**
show smtp	P	Show the information of SMTP	switch#**show smtp**
no smtp	G	Disable SMTP function	switch(config)#**no smtp**
event device-cold-start [Disable|Systemlog|SMTP|Both]	G	Set cold start event type	switch(config)#**event device-cold-start both**

event device-warm-start [Disable|Systemlog|SMTP|Both]	**G**	Set warm start event type	switch(config)#**event device-warm-start both**
event authentication-failure [Disable|Systemlog|SMTP|Both]	**G**	Set Authentication failure event type	switch(config)#**event authentication-failure both**
event ring-topology-change [Systemlog|SMTP|Both]	**G**	Set X-ring topology changed event type	switch(config)#**event ring-topology-change both**
event systemlog [Disable|Link-UP|Link-Down|Both]	**I**	Set port event for system log	switch(config)#**interface fastethernet 2** switch(config-if)#**event systemlog both**
event smtp [Disable|Link-UP|Link-Down|Both]	**I**	Set port event for SMTP	switch(config)#**interface fastethernet 2** switch(config-if)#**event smtp both**
show event	**P**	Show event selection	switch#**show event**
no event device-cold-start	**G**	Disable cold start event type	switch(config)#**no event device-cold-start**
no event device-warm-start	**G**	Disable warm start event type	switch(config)#**no event device-warm-start**
no event authentication-failure	**G**	Disable Authentication failure event type	switch(config)#**no event authentication-failure**
no event ring-topology-change	**G**	Disable super ring topology changed event type	switch(config)#**no event ring-topology-change**
no event systemlog	**I**	Disable port event for system log	switch(config)#**interface fastethernet 2** switch(config-if)#**no event systemlog**

no event smtp	**I**	Disable port event for SMTP	switch(config)#**interface fastethernet 2** switch(config-if)#**no event smtp**
show systemlog	**P**	Show system log client & server information	switch#**show systemlog**

SNTP Commands Set

Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#**sntp enable**
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight**
sntp daylight-period [Start time] [End time] Format:[yyyymmdd-hh:mm]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)#**sntp daylight-period 20060101-01:01 20060202-01-01**
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight-offset 3**
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp ip 192.169.1.1**
sntp timezone [Timezone] Format: [1~63]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#**sntp timezone 22**
show sntp	P	Show SNTP information	switch#**show sntp**
show sntp timezone	P	Show index number of	switch#**show sntp timezone**

		time zone list	
no sntp	**G**	Disable SNTP function	switch(config)#**no sntp**
no sntp daylight	**G**	Disable daylight saving time	switch(config)#**no sntp daylight**

X-Ring Commands Set

Commands	Level	Description	Example
ring enable	**G**	Enable X-ring	switch(config)#**ring enable**
ring master	**G**	Enable ring master	switch(config)#**ring master**
ring ringport **[1st Ring Port] [2nd Ring Port]**	**G**	Configure 1st/2nd Ring Port	switch(config)#**ring ringport 7 8**
ring couplering	**G**	Enable couple ring	switch(config)#**ring couplering**
ring couplingport **[Coupling Port]**	**G**	Configure Coupling Port	switch(config)#**ring couplingport 1**
ring controlport **[Control Port]**	**G**	Configure Control Port	switch(config)#**ring controlport 2**
ring dualhoming	**G**	Enable dual homing	switch(config)#**ring dualhoming**
ring homingport **[Dual Homing Port]**	**G**	Configure Dual Homing Port	switch(config)#**ring homingport 3**
show ring	**P**	Show the information of X-Ring	switch#**show ring**
no ring	**G**	Disable X-ring	switch(config)#**no ring**
no ring master	**G**	Disable ring master	switch(config)#**no ring master**
no ring couplering	**G**	Disable couple ring	switch(config)#**no ring couplering**
no ring dualhoming	**G**	Disable dual homing	switch(config)#**no ring dualhoming**

LLDP Command Set

Commands	Level	Description	Example
lldp enable	**G**	Enable LLDP function	switch(config)#**lldp enable**
lldp interval [TIME sec]	**G**	Configure LLDP interval	switch(config)#**lldp interval 10**
no lldp	**G**	Disable LLDP function	switch(config)#**no lldp**
show lldp	**P**	Show LLDP function	switch#**show lldp**

Access Control List Command Set

Commands	Level	Description	Example
acl gid [Group ID]	G	Configure ACL group id	switch(config)#**acl gid 1**
acl action [Permit|Deny]	G	Configure ACL action	switch(config)#**acl action permit**
acl vid [Any|VLAN ID]	G	Configure ACL VLAN ID	switch(config)#**acl vid any**
acl pktype [IPv4|Non-IPv4]	G	Configure ACL packet type	switch(config)#**acl pktype ipv4**
acl ethtype [Any|ARP|IPX|Type value]	G	Configure ACL ether type	switch(config)#**acl ethtype arp**
acl sip any	G	Any Src IP	switch(config)#**acl sip any**
acl sip ip [IP address][Mask]	G	Specify Src IP and Mask	switch(config)#**acl sip ip 192.168.1.1 255.255.255.0**
acl dip any	G	Any Des IP	switch(config)#**acl dip any**
acl dip ip [IP address][Mask]	G	Specify Des IP and Mask	switch(config)#**acl dip ip 192.168.1.1 255.255.255.0**
acl frg [Check|Uncheck]	G	Configure ACL IP fragment	switch(config)#**acl frg check**
acl l4 other [Any|ICMP|IGMP|Protocol value]	G	Configure ACL L4 protocol other type	switch(config)#**acl l4 other any**
acl l4 tcp [Any|FTP|HTTP|Port Number]	G	Configure ACL L4 protocol TCP	switch(config)#**acl l4 tcp ftp**
acl l4 udp [Any|TFTP|Port Number]	G	Configure ACL L4 protocol UDP	switch(config)#**acl l4 udp tftp**
acl add	G	Add new group structure	switch(config)#**acl add**
acl show	G	Show content of	switch(config)#**acl show**

		current configured ACL group.	
acl test [number]	**G**	Debug command for ACL.	switch(config)#**acl test 0**
no acl	**G**	Delete ACL group.	switch(config)#**no acl 1**
show acl	**P**	Show ACL list.	switch#**show acl**